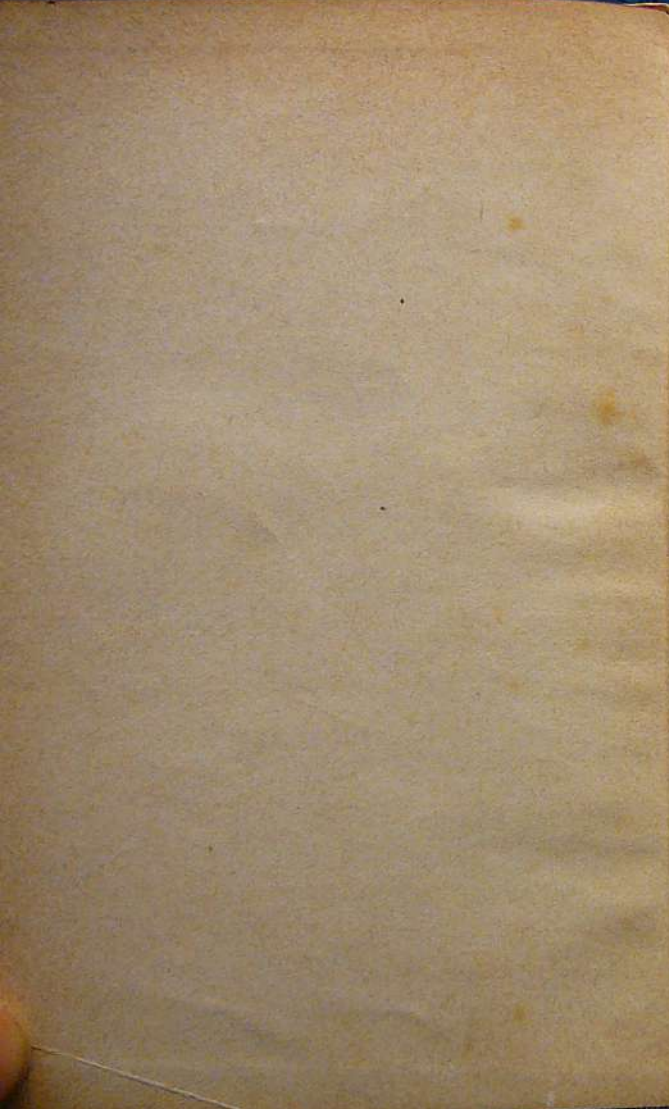
MANUALI HOEPLI

MARIO ZANOTTI

CRITTOGRAFIA

LE SCRITTURE SEGRETE

MILANO - ULRICO HOEPLI - EDITORE

CRITTOGRAFIA

MANUALI HOEPLI

MARIO ZANOTTI

CRITTOGRAFIA

Le Scritture Segrete

ULRICO HOEPLI
EDITORE-LIBRAIO DELLA REAL CASA
MILANO
1928

INDICE DELLA MATERIA

PARTE I

GENERALITÀ

PARTE II

LE SCRITTURE CIFRATE

PARTE III

LE SCRITTURE DISSIMULATE O CONVENZIONALI E LE SCRITTURE INVISIBILI

BIBLIOGRAFIA

BAZERIES, *Les chiffres de Napoléon I pendant la campagne de 1813*, Fontainebleu, 1896.

COLLON, *Etude sur la cryptographie* (Revue de l'Armée Belge, vol. 24, 25, 26, 27, 28).

DELASTELLE, *Traité élémentaire du cryptographie*, Parigi, 1920.

DROSCHER, *Die Methoden der Geheimschriften*, Leipzig, 1921.

DE VIARIS, *Cryptographie*, Parigi, 1888.

— *L'art de chiffrer et déchiffrer les depêches secrètes*, Parigi, 1893.

GIOPPI, *La crittografia*, Hoepli, 1896.

GABRIELLI (ABATE PIER DOMENICO), *Crittografia fiorentina* (R. Archivio di Firenze).

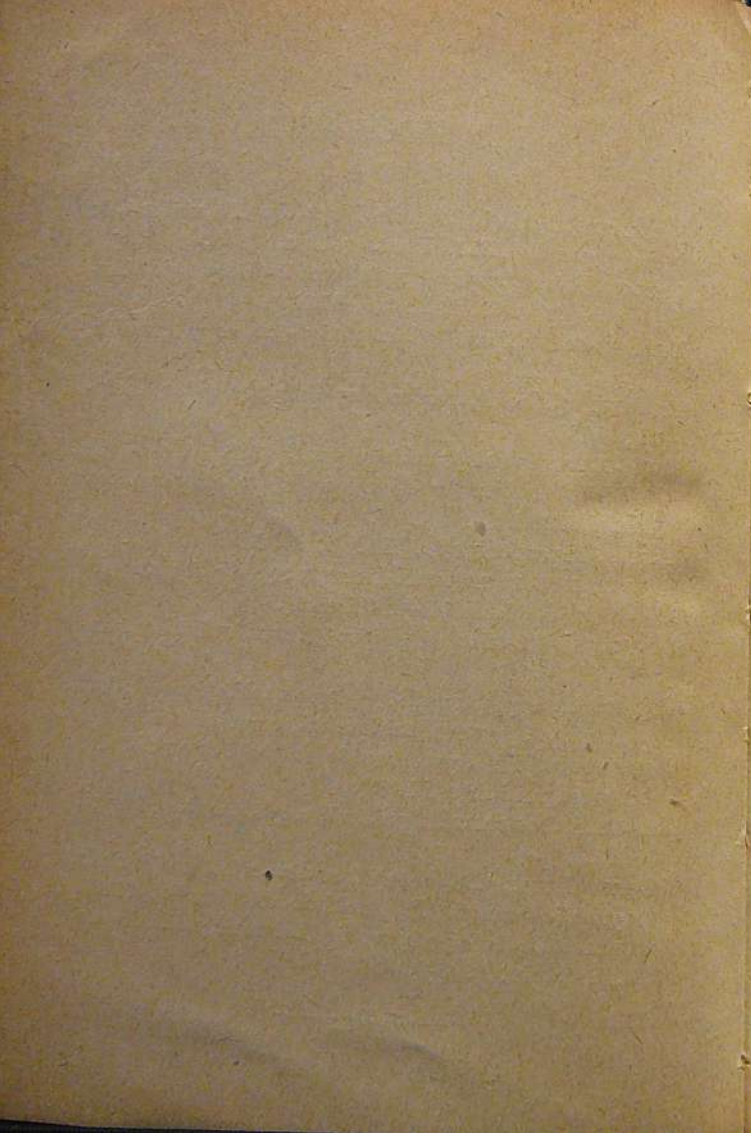
GIVIERGE, *Question de chiffre* (Revue militaire francaise, 1924).

JOSSE, *La cryptographie et ses applications à l'art militaire* (Revue maritime et coloniale, 1885).

KERCHOFFS, *La cryptographie militaire* (Journal des sciences militaires, 1883).

LANGE E SOUDART, *Traité de cryptographie*, Parigi, 1925.

PASINI LUIGI, *Delle scritture in cifra usate dalla repubblica veneta* (R. Archivio di Venezia, 1873).

VALERIO, *De la cryptographie* (Librairie militaire de L. Baudoin, 1893-96).

PREFAZIONE

Questo lavoro viene a reintegrare nella collezione dei duemila Manuali Hoepli uno di questi da tempo esaurito e, sia lecito dirlo, superato da molte innovazioni introdotte nell'arte crittografica.

Dal 1897, data della prima pubblicazione del Manuale di Crittografia del Gioppi, ad oggi molte esperienze, specie durante la grande guerra, e molte nuove applicazioni si son fatte in materia di scritture segrete, era quindi necessario colmare il vuoto, nell'interesse degli uomini di studio e di lavoro, fedeli lettori della serie enciclopedica dei Manuali.

Il manuale corredato da un'estesa bibliografia, non vuol essere un trattato completo, chè la mole non lo consentirebbe, ma aspira soltanto ad essere una guida per coloro che vogliono dedicarsi a questi studi o che amano conoscere una branca tanto importante dell'attività politica, militare e commerciale. Con rendimento inoltre potrà essere consultato dai dirigenti delle organizzazioni che oggi fanno largo uso della critto-

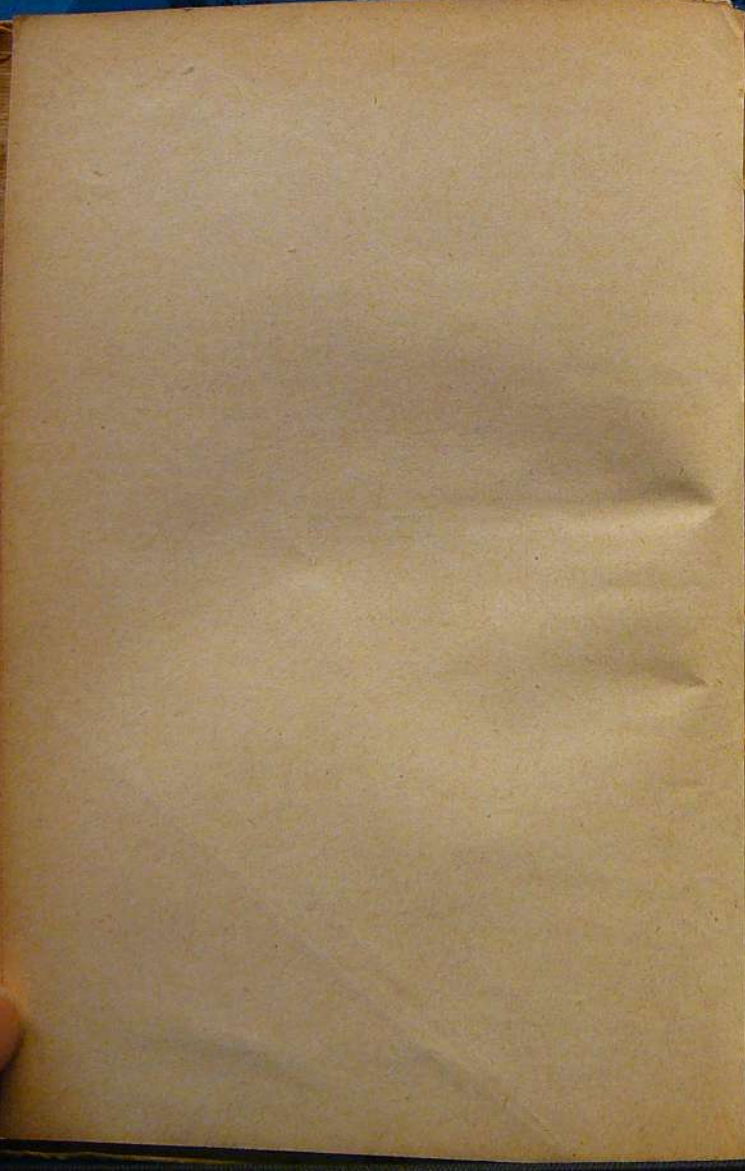
grafia, e che soventi devono affidarsi a pareri di empirici o di affaristi, rischiando di esporre delicate questioni alla mercè di chiunque abbia interesse a profittarne.

Nella compilazione del Manuale, ho tratto, per sua benevola concessione, preziosissimi e numerosi dati dagli insegnamenti e dai lavori originali del Comm. Luigi Sacco, mio primo Maestro e guida nello studio di questa materia. — A Lui sono dovute geniali concezioni di metodi di cifratura e nuovi procedimenti di decrittazione.

Al Comm. Sacco quindi deve giungere la riconoscenza dei lettori e mia, perchè l'ordinamento veramente scientifico del materiale crittografico, quale oggi in Italia ci è dato sfruttare, è opera da considerarsi essenzialmente sua.

L'Autore

PARTE PRIMA

GENERALITÀ

CAPITOLO I.

La crittografia

La crittografia è l'arte delle scritture segrete, etimologicamente deriva dalle parole greche *Kriptos*: nascosto, e *graphos*: scrittura.

Le scritture segrete di cui essa si occupa possono raggrupparsi in tre tipi fondamentali:

le scritture invisibili;
le scritture dissimulate o convenzionali;
le scritture cifrate.

Le prime si ottengono vergando le corrispondenze con inchiostri invisibili, detti anche inchiostri simpatici, non appariscenti ad un esame superficiale, ma che si rivelano soltanto in seguito all'azione di un particolare reagente, noto al destinatario della corrispondenza.

Le seconde consistono nell'impiego di un linguaggio nel quale si cerca di mantenere l'apparenza del linguaggio normale, attribuendo ai varî vocaboli usati un significato convenzionale, oppure diluendo in un testo normale i varî elementi che

devon formare le lettere o le parole del testo segreto.

Questi due tipi di scrittura sono impiegati essenzialmente nelle corrispondenze per scopi di spionaggio politico o militare e per scopi rivoluzionari.

Le scritture cifrate propriamente dette, delle quali tratteremo ampiamente, sono costituite da testi aventi nettamente l'aspetto di linguaggio segreto e incomprensibile a chi non conosca la convenzione, o cifra, necessaria per la loro intelligenza.

Prima di entrare nel vivo dell'argomento è opportuno premettere alcune definizioni di termini che saranno frequentemente impiegati, la cui conoscenza gioverà alla esatta comprensione dell'argomento.

Cifrare significa tradurre un testo chiaro in linguaggio cifrato, valendosi di regole o di documenti conosciuti o posseduti da due o più corrispondenti.

Decifrare è l'operazione inversa, compiuta servendosi di tali mezzi regolarmente posseduti.

Decrittare (o *decriptare*) è l'operazione equivalente al decifrare, ma fatta da chi non sia il destinatario della comunicazione cifrata e senza il possesso regolare delle regole o dei documenti.

Si dice *crittogramma* o testo cifrato, il testo risultante dopo compiuta l'operazione del cifrare.

Cifrario è l'insieme delle regole e dei documenti occorrenti per cifrare, e per decifrare, può essere costituito da semplici tabelle o da grossi volumi.

Chiave (o *cifra*) è una convenzione particolare consistente in una parola o in una frase, facilmente

ritenibile a memoria, che serve direttamente a eseguire la cifratura o ne è un accessorio.

A stretto rigore dovrebbero comprendersi nello studio della crittografia altresì le iscrizioni composte con figure, o con simboli, ma poichè tra i Manuali Hoepli già esiste il « *Dizionario illustrato dei simboli* » di G. Ronchetti, che magistralmente e ampiamente sviluppa tale argomento, ci dispensiamo dal trattarne nel presente volume.

CAPITOLO II.

La crittografia nella storia, nell'arte, nella letteratura, nel commercio, nella guerra attraverso i secoli

Sebbene tutti intuiscano l'importanza dell'arte crittografica e la sua innegabile influenza, per quanto occulta, sulla vita dei popoli, non ci sembra tuttavia inutile illustrarne brevemente l'impiego e lo sviluppo attraverso i secoli, onde farne apprezzare il valore e la portata.

Cenni storici.

Si può senza dubbio affermare che la necessità di corrispondere con scritture segrete è antica quanto l'uomo e che la crittografia è stata in ogni tempo strettamente legata alla storia politica e militare dei diversi paesi.

Pur avendo motivo di supporre che nelle antiche civiltà Cinesi, Persiane e Cartaginesi fossero impiegati questi mezzi, non sono giunti sino a noi documenti che ce lo confermino. — All'opposto

notizie certe dell'uso corrente di procedimenti crittografici presso i Greci ed i Romani si trovano in varî autori: Erodoto, Polibio, Plutarco, Svetonio, Aulo Gellio, ecc.

Plutarco, ad esempio, descrive la scytala degli Spartani, asticciuola costruita in due esemplari di dimensioni identiche, sulla quale si avvolgeva una listerella di pergamena e quindi lungo le generatrici si scriveva il messaggio. Veniva poi svolto e spedito al corrispondente che con operazione inversa poteva leggerlo rimettendolo nella posizione eguale a quella iniziale. La scytala veniva costruita in due esemplari quando un generale partiva per una spedizione, un esemplare veniva conservato dai Governanti e l'altro consegnato al Generale.

Svetonio, nella vita di dodici Cesari, ha descritto l'alfabeto di cui si valeva Giulio Cesare per corrispondere coi suoi luogotenenti. Può considerarsi il primo vero sistema di scrittura cifrata usato: consisteva nel sostituire a ogni lettera del testo chiaro la lettera corrispondente presa in un alfabeto ordinario, ma spostato di quattro posti rispetto a quello normale.

Nel medio evo presso le Corti Papale e dei principi italiani l'arte crittografica fu molto coltivata; della fine di questo periodo (sec. XV) sono infatti il primo manuale di cifratura conosciuto, dell'Alberti, segretario alle cifre presso la curia romana, ed il primo trattato di decrittazione di Cicco Simonetta, addetto alla Cancelleria degli Sforza.

Specialmente nel Rinascimento la crittografia ebbe un notevole impulso, soprattutto per opera

degli italiani Cardano e Porta e del francese Vigenère, vissuti nel secolo XVI. Di questo periodo si possiedono numerosi documenti, che possono ancor oggi considerarsi utilissimo materiale di studio.

Fin dal secolo XVII la Repubblica Veneta aveva organizzato un servizio di cifratura, posto alla diretta dipendenza del Consiglio dei dieci e costituito da Segretari addetti alle cifre, alcuni dei quali erano abilissimi; del pari ottimo personale trovavasi alla Corte papale ed a quella di Enrico IV.

È appunto nel secolo XVII che la crittografia ha raggiunto i perfezionamenti più importanti, forse ancor oggi non superati, per merito di molti ingegni che vi si dedicarono con passione e perseveranza; basti citare Bacone e Rossignol, la cui abilità nel decrittare ne fece fin anco dare per traslato nella lingua francese il nome al grimaldello.

Del pari di questo tempo, sotto il regno di Luigi XIV, è l'istituzione presso il Ministero della Guerra francese, per opera del Luvois, del primo servizio regolare di cifratura, mediante cifrari costruiti con una cura ed una perfezione che non si ritroverà più che ai nostri giorni.

All'opposto il secolo XVIII e la prima metà del XIX segnano la decadenza della crittografia, la quale venne pur sempre impiegata, ma con metodi deboli e poco curati.

Anche negli eserciti di Napoleone I la cifratura venne usata con trascuratezza, tanto che è ormai accertato che la serie dei rovesci subiti da Napoleone in Russia è dovuta in parte alla debolezza dei

sistemi di cifratura, che venivano continuamente svelati dai Russi.

Danni consimili derivarono all'Esercito francese nella guerra del 1870-71 per le deficienti precauzioni adottate nell'uso della cifratura.

Si può ritenere che il 1880 segni l'epoca del risveglio degli studi crittografici, s'inizia una nuova êra nella quale le applicazioni dell'arte crittografica si moltiplicano e si perfezionano, si compiono e pubblicano accurati studi con carattere veramente scientifico e generale; in molte scuole militari si insegna ufficialmente la crittografia.

Venne infine la grande guerra 1914-1918, che, come in tutti i rami dell'attività umana, portò anche un enorme accrescimento delle necessità di impiegare i procedimenti crittografici e di impiegarli con sistemi che dessero le maggiori garanzie per la loro inviolabilità.

Tale necessità era resa ancor più forte dal largo uso della radiotelegrafia che, come è noto, ha il gravissimo difetto della facile intercettabilità, e richiede quindi che i dispacci venuti in possesso degli avversari non possano essere decrittati assolutamente, o quanto meno richiedano un lunghissimo lavoro, che faccia oltrepassare i limiti di tempo utili per lo sfruttamento delle notizie così raccolte.

Di conseguenza ogni Governo ed ogni Esercito in lotta perfezionarono con somma alacrità i sistemi di cifratura e impiegarono valenti operatori per scoprire i sistemi usati dai nemici.

Larga messe d'esperienza è perciò stata raccolta

in quel periodo, ma essa è rimasta patrimonio di pochi, mentre sarebbe di somma utilità, come vedremo, che l'arte crittografica avesse numerosi cultori per le molteplici applicazioni che può avere negli svariati campi delle umane attività.

Le applicazioni della crittografia.

Abbiamo constatato esaurientemente come quest'arte sia in ogni tempo stata in onore; vedremo come estese siano state le sue applicazioni e come ancor oggi possano divenirlo.

L'esperienza dell'ultima guerra ha ampiamente dimostrato come l'arte militare non possa esimersi dal fare ricorso a tutte le risorse dell'arte del cifrare. Gli ordini dei comandi delle piccole e delle grandi unità d'un esercito esigono rapidità e segretezza, a tal fine nessun mezzo migliore si può avere a disposizione all'infuori del telegramma in cifra.

E l'arte crittografica nella branca della decrittazione può rendere inoltre enormi servizi agli eserciti nei periodi di guerra, quando sia sfruttata per interpretare gli innumerevoli dispacci che gli avversari si scambiano per telefono e per telegrafo da un estremo all'altro dei fronti, nell'interno e tra i varî teatri d'operazione, soprattutto i radiotelegrammi forniscono larga messe per questo lavoro di scoperta.

Nei periodi di pace, di normale attività dei popoli, la situazione si modifica: il telegrafo lavora

per i Ministeri e per le grandi organizzazioni finanziarie e industriali, la diplomazia e la finanza internazionale hanno influenza preponderante nella vita sociale rispetto alle necessità dell'arte militare.

Il campo nel quale normalmente le corrispondenze cifrate sono impiegate nella più larga misura ed in ogni tempo è evidentemente la corrispondenza diplomatica: tutta la diplomazia segreta del passato, sino alla fine del sec. XVII, è basata sull'uso della crittografia ed anche oggi innumerevoli sono i telegrammi per filo e per radio che quotidianamente i Governi del mondo intero scambiano coi proprî agenti.

Ogni Ministero d'ogni paese ha personale apposito, esclusivamente incaricato della corrispondenza cifrata coll'estero e coll'interno, che lavora incessantemente; e questa istituzione abbiamo visto datare fino dal XV secolo, quando ogni governo cominciò ad avere proprî segretari alle cifre

Attualmente molte grandi banche europee ed americane, seguendo l'evoluzione del dopo guerra, conseguenza dell'intensificarsi e dell'estendersi delle relazioni coll'estero, sono state indotte a costituirsi degli uffici cifra, per mantenere segrete le grandi operazioni finanziarie, onde lottare contro la concorrenza ed evitare pericolose ripercussioni sull'opinione pubblica.

Le grandi compagnie esercenti le reti radiotelegrafiche, poi, data la caratteristica già accennata di questo mezzo di trasmissione, cioè la piena possibilità di essere intercettate, hanno dovuto cer-

care di tenere celato agli indiscreti il contenuto dei dispacci che loro sono affidati.

Volendo perciò offrire ai proprî clienti la stessa sicurezza date dalle amministrazioni dei telegrafi ordinari, dove le comunicazioni per filo sono conosciute soltanto da impiegati vincolati dal segreto professionale, le compagnie di radiotelegrafia hanno adottato l'uso generale di cifrare tutte le comunicazioni prima di lanciarle nello spazio, le compagnie quindi non soltanto usano costantemente ottimi sistemi crittografici, ma hanno già cominciato ad impiegare macchine per cifrare automaticamente, delle quali tratteremo a suo tempo.

Ma non soltanto nel dominio della politica e degli affari si è fatto sentire il bisogno di utilizzare nella più larga misura le cognizioni sui linguaggi segreti, anche gli storici hanno dovuto ricercare il concorso, non tanto dei sistemi di cifratura, quanto dell'arte della decrittazione.

Quest'arte è destinata ad aprire agli storici la via a nuove indagini su avvenimenti rimasti finora inspiegati, come il mistero della Maschera di Ferro, che ha appassionato numerosi studiosi e di cui una soluzione è stata prospettata soltanto due secoli più tardi da un crittologo che lavorava a ricerche relative alle campagne del Catinat in Piemonte.

Più recentemente studi compiuti da specialisti sulle opere di Bacone, che si sapeva essere l'inventore di un sistema crittografico, hanno permesso di chiarire in parte un periodo della storia d'Inghilterra rimasto fin ora oscuro e di portare elementi decisivi alla soluzione dell'appassionante questione

dell'identità di Bacone e di Shakeaspeare. Chi voglia attingere maggiori notizie su questo argomento potrà consultare gli studi dell'americano Cartier pubblicati nel *Mercure de France*, n. 563 del 1921; 568, 584 e 582 del 1922; 591, 596 e 601 del 1923.

Financo i romanzieri hanno fatto ricorso alla crittografia per rendere più vive ed appassionanti le loro opere, come si può constatare nello *Scarabeo doro* di Edgardo Poë; nella *Fisiologia del matrimonio* e nella *Storia dei Tredici di* Onorato Balzac; in *Mattia Sandorf*, in *La Jangada*; nel *Viaggio al centro della Terra* di Giulio Verne; nei *Compagni del Silenzio* di Paolo Féval, ed in molti altri lavori.

Aggiungeremo ancora come congiurati, cospiratori ed anarchici si siano valsi in ogni epoca di linguaggi segreti per le loro macchinazioni.

Per rendere infine evidenti gli incommensurabili danni che possono derivare ad una nazione dalla trascuranza degli studi e delle applicazioni razionali della crittografia riporteremo un episodio rivelato nelle memorie di Falkenhayn sulla guerra mondiale.

Sono noti, almeno nelle linee generali, gli avvenimenti che condussero alla strepitosa vittoria dei tedeschi sui russi a Tannenberg alla fine dell'agosto 1914.

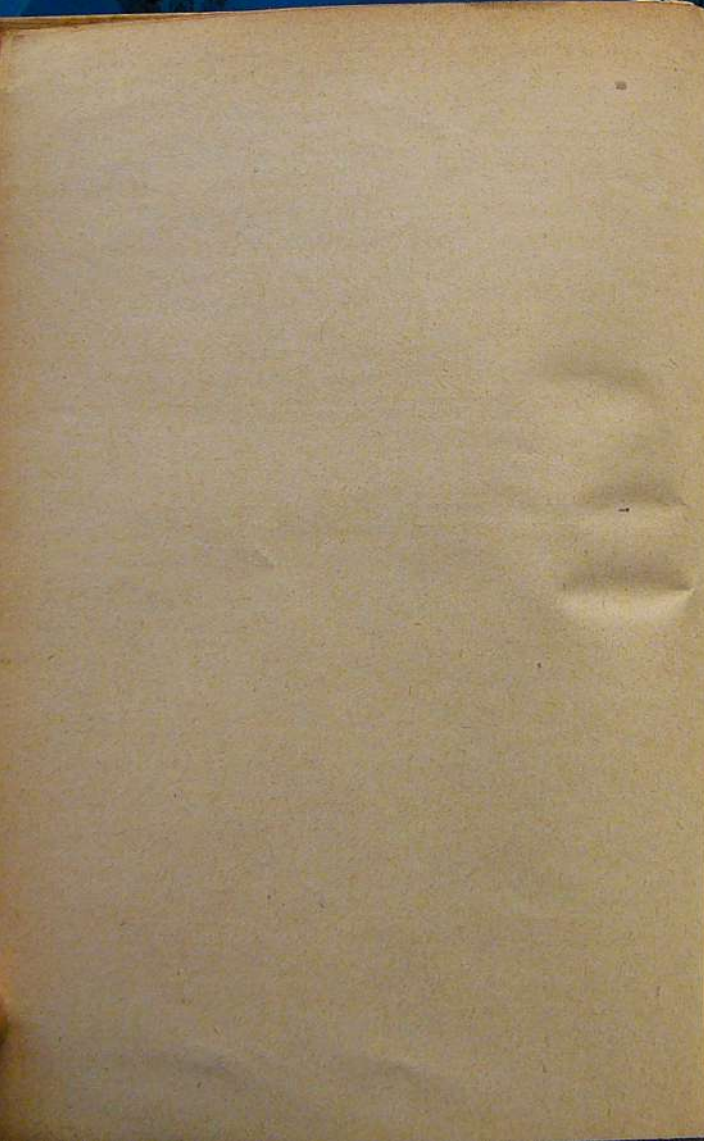
Ludendorff racconta tali avvenimenti per disteso nelle sue memorie, ma tace un particolare che semplificava assai il suo compito e diminuisce

alquanto la sua fama d'audace. Egli conosceva il cifrario impiegato dai russi; essendo nelle armate dei suoi avversari tutti gli ordini diramati per mezzo della radiotelegrafia, egli li riceveva, li decifrava e li conosceva nello stesso istante degli esecutori, quindi conosceva intenzioni e mosse dei nemici ed in conseguenza regolava meditatamente ogni sua azione.

Il Falkenhayn nel riferire l'episodio, aggiunge che tutte le sere i radiotelegrammi intercettati erano decifrati verso le ore 23; quando eccezionalmente v'era qualche ritardo Ludendorff giungeva inquieto all'ufficio cifra per saperne la ragione.

Sinteticamente tracciata la realtà storica e possibilità applicativa dell'arte crittografica, vediamo i più importanti sistemi nella loro struttura e nel loro impiego.

PARTE SECONDA

LE SCRITTURE CIFRATE

CAPITOLO III.

Le caratteristiche delle scritture cifrate

Come abbiamo detto le scritture cifrate sono quelle che si presentano sotto l'aspetto evidente di linguaggio segreto, in una successione incoerente di segni (usualmente lettere o numeri) variamente raggruppati non aventi un significato comprensibile.

Le operazioni per tradurre un testo chiaro in un testo cifrato si possono raggruppare in due tipi principali:

la *trasposizione*, cioè l'operazione mediante la quale gli elementi di un testo chiaro vengono cambiati di posto, ossia trasposti, secondo una regola stabilita in modo che la ricostruzione del testo chiaro non sia possibile a chi non conosca quella regola;

la *sostituzione*, cioè l'operazione con la quale gli elementi del testo chiaro vengono sostituiti con altri elementi secondo apposite regole, note ai corrispondenti.

Le due operazioni si possono applicare una o più

volte, separatamente o cumulativamente. Gli elementi del testo chiaro sui quali si eseguisce la trasposizione o la sostituzione possono essere: lettere semplici, sillabe, gruppi di due o più lettere, parole, frasi od anche frazioni di lettera.

È poi entrata nell'uso generale una classificazione dei sistemi di cifratura, per cui questi si dividono in:

sistemi letterali, quelli nei quali gli elementi su cui si compiono le operazioni di cifratura sono lettere (o numeri), o frazioni di lettere (o di numeri), od al massimo gruppi di lettere (o di numeri);

sistemi a repertorio, quelli nei quali si eseguisce su lettere o numeri, o sillabe, o parole, o intere frasi una semplice operazione di sostituzione, che può essere o no seguita da ulteriori operazioni di cifratura (sopracifratura).

CAPITOLO IV.

I SISTEMI DI CIFRATURA LETTERALE

I. — *Operazioni preliminari.*

Per compiere le operazioni di cifratura coi sistemi letterali occorre conoscere cosa siano l'omogeneità dei gruppi cifrati e le chiavi di cifratura e come si ottengano.

Nei sistemi di cifratura letterale vengono alterate le lettere dei testi chiari ottenendo crittogrammi costituiti da gruppi di lettere e di numeri non aventi significato comprensibile. Se i crittogrammi dovessero essere trasmessi come corrispondenza ordinaria non vi sarebbe alcun inconveniente che il testo cifrato fosse costituito da lettere piuttosto che da numeri, anche frammischiati, o da qualsiasi altro segno, ma ciò non può ammettersi quando i crittogrammi devono trasmettersi per telegrafo con filo o senza, come avviene nel caso più comune.

In questo caso è necessario che i gruppi sian *omogenei*, per evitare errori di trasmissione, cioè siano

costituiti da gruppi aventi un numero possibilmente costante di sole lettere o di soli numeri, escluso qualsiasi altro segno nonchè il frammischiamento di lettere e di numeri (1).

Normalmente le lettere od i numeri saranno a gruppi di cinque, tale essendo il massimo concesso dalle convenzioni telegrafiche internazionali (2), perchè i gruppi stessi possano essere tassati per una sola parola, e dato che l'esperienza ha dimostrato che il personale telegrafista trasmette senza errori e con rapidità testi cifrati quando i gruppi senza significato apparente che li costituiscono sono omogenei e costituiti di cinque segni (lettere o numeri). Per ottenere dunque che i gruppi cifrati siano omogenei è sovente necessario nei sistemi letterali tradurre in lettere i numeri ed i principali segni d'interpunzione nei testi chiari.

Un modo semplice per sopperire a questa necessità consiste nello stabilire una particolare convenzione del tipo della seguente.

Osservando che nella lingua italiana le lettere K, W, X, Y sono raramente impiegate si conviene che nel caso un testo chiaro contenga numeri o segni di interpunzione debba venire modificato, usando i seguenti accorgimenti, prima di essere cifrato:

1.° i numeri siano fatti precedere e seguire dalla lettera W e sostituiti da lettere dell'alfabeto,

---

(1) Vedi *Appendice*: « Disposizioni internazionali relative ai telegrammi redatti in linguaggio segreto ».
(2) Idem.

per esempio:

1 = A, 2 = B, 3 = C, 4 = D, 5 = E, 6 = F, 7 = G, 8 = H, 9 = I, O = J;

2.º la virgola ed il punto siano sostituiti rispettivamente dalle lettere X ed Y;

3.º laddove le lettere W, X ed Y debbano mantenere il loro suono reale, invece di quello convenzionale stabilito, siano precedute dalla lettera K (il cui suono in italiano può essere rappresentato con C H).

Con tale convenzione i numeri e i segni d'interpunzione saranno cifrati come le altre lettere del testo chiaro e daranno luogo a gruppi cifrati omogenei con quelli derivanti dalle altre lettere chiare.

Se ad esempio si dovesse cifrare:

« Noto agente Wolff offre merce 45,78 »

si trasformerebbe prima così:

Noto agente KWolff offre merce WDEXGHW, ottenendosi in tal modo un testo in lettere, cioè omogeneo.

Nei sistemi letterali generalmente il segreto è affidato ad una *chiave*, cioè ad una parola o frase convenzionale, facilmente ritenibile a memoria, che serve a compiere direttamente le operazioni di cifratura o che ne è un accessorio.

Le chiavi possono essere soltanto mnemoniche, cioè nomi proprî o comuni, o frasi come: Giacomo, Ferrara; carretto; quando Giason dal Pelio; ecc.; oppure possono essere numeriche ed in questo caso sono ricavate da una chiave mnemonica, per ovvia comodità. La trasformazione di una chiave

mnemonica in numerica si effettua numerando successivamente le lettere della chiave mnemonica secondo l'ordine nel quale si incontrano nell'alfabeto normale della lingua; per esempio:

F O R L Ì; C A S A L P U S T E R L E N G O
1 4 5 3 2; 3 1 13 2 7 11 16 14 15 4 12 8 5 9 6 10

Vedremo in seguito l'impiego pratico delle chiavi nella cifratura.

II. — *Sistemi letterali di cifratura a trasposizione.*

I sistemi di cifrare per trasposizione sono molti, con questi si disordinano le lettere del testo chiaro in modo da ottenere un crittogramma nel quale esse risultino in un ordine diverso da quello normale.

Di tali sistemi ve ne sono alcuni troppo ingenui ed altri troppo complessi, in pratica quelli adottabili si riducono ai seguenti:

trasposizione semplice,
» con chiave,
» doppia,
» con griglie,
» con figure.

Trasposizione semplice.

Per usare questo modo di cifratura si adopera un foglio di carta quadrettata e si conviene tra i corrispondenti di usare un determinato numero di quadretti per ciascuna riga orizzontale. Il

testo chiaro si scrive riga per riga, mettendo una lettera per ogni casella ed impegnando per ogni riga il numero di caselle convenuto; quindi per ottenere il crittogramma si rilevano le lettere inserite nelle varie caselle in un modo prestabilito, che può essere: per colonne dalla destra o dalla sinistra, per diagonali partendo da uno qualunque dei vertici, ecc.

Se il numero delle lettere del testo chiaro non fosse un multiplo del numero delle caselle orizzontali adoperate, si può operare in due modi: o riempire le caselle che restano vuote nell'ultima riga con lettere qualunque, o lasciare vuote le caselle stesse. Per decifrare un crittogramma compilato col sistema di cui diciamo si opera in questo modo: si contano le lettere contenute nel crittogramma, si divide questo numero per quello delle caselle che si è convenuto di adoperare in ciascuna riga; il numero così ottenuto indicherà il numero di righe che si devono adoperare per eseguire la decifrazione del testo ricevuto.

Si scrivono quindi in un foglio quadrettato, delle dimensioni determinate (larghezza convenuta e altezza ottenuta colla divisione predetta) successivamente le lettere del crittogramma nell'ordine concordato (colonne, diagonali, ecc.).

Nel caso il rettangolo debba risultare incompleto il destinatario prima di inscriverví il crittogramma annullerà le caselle che non devono essere usate, giusta gli accordi stabiliti pel modo di scritturazione dei testi chiari.

Si debba per esempio cifrare il testo chiaro:

« Seduta odierna parlamento votato aumento tariffe doganali »;

avendo convenuto di usare nove caselle per ogni riga, lo si prepara in questo modo:

S	E	D	U	T	A	O	D	I
E	R	N	A	P	A	R	L	A
M	E	N	T	O	V	O	T	A
T	O	A	U	M	E	N	T	O
T	A	R	I	F	F	E	D	O
G	A	N	A	L	I			

e rilevandolo per colonne dalla destra si otterrà:

1.° I A A O O = D L T T D = O R O N E = A A V E F = I T P O M = F L U A T = U I A D N = N A R N E = R E O A A = S E M T T = G

rilevandolo invece per diagonali dal vertice in alto a destra:

2.° I D A O L = A A R T O = T A O T O = U P V N D = D A O E E = E N T M F = S R N U F = I E E A I = L M O R A = T A N T A = G

Il 1° ed il 2° modo di rilevamento danno il crittogramma pronto per la trasmissione a gruppi di cinque lettere.

Trasposizione con chiave.

Per cifrare per trasposizione servendosi d'una chiave il procedimento da usare è analogo al precedente. La chiave mnemonica, che si stabilisce tra i corrispondenti, serve ad indicare il numero di caselle che si devono usare per ciascuna riga orizzontale, ed inoltre, mediante la trasformazione in chiave numerica che sempre si deve fare, serve ad indicare l'ordine nel quale si deve effettuare il rilevamento del crittogramma. Tale ordine è indicato dall'ordine naturale dei numeri della chiave numerica, ossia si comincerà a rilevare dalla colonna segnata dal n. 1 e poi si passerà alle altre numerate 2, 3, ecc.

Per decifrare basterà dividere il numero delle lettere del crittogramma ricevuto per quello delle lettere componenti la chiave, ottenendosi così il numero delle righe da impiegare; il crittogramma verrà quindi scritto per colonna secondo l'ordine indicato dalla chiave numerica, tenendo conto delle caselle che eventualmente dovranno rimanere vuote, se il numero delle lettere del crittogramma non è un multiplo del numero delle lettere della chiave.

Ad esempio si debba cifrare il testo chiaro:

« Acquistate 500 Banca Italia Ricci »

con la chiave: Vercelli; il testo chiaro, contenendo un numero, dovrà prima essere reso omogeneo, secondo quanto abbiamo visto, così:

« Acquistate WEJJW Banca Italia Ricci »
indi si preparerà la seguente tabella:

chiave mnemonica:	V E R C E L L I
chiave numerica :	8 2 7 1 3 5 6 4
Testo chiaro	A C Q U I S T A
	T E W E J J W B
	A N C A I T A L
	I A R I C C I

dalla quale rilevando per colonne nell'ordine indicato dalla chiave numerica si otterrà il crittogramma:

U E A I C = E N A I J = I C A B L = S J T C T = W A I Q W = C R A T A = I

Doppia trasposizione.

La cifratura per trasposizione si può effettuare anche due volte di seguito, eseguendola la prima volta sul testo chiaro e la seconda volta sul crittogramma ottenuto colla prima cifratura.

Per decifrare in questo caso si dovranno eseguire successivamente le operazioni esposte precedentemente.

Trasposizione con griglie.

Di griglie per cifrare per trasposizione ne sono state immaginate moltissime, diremo qualcosa soltanto di quelle quadrate, o a rotazione, e di quelle indefinite.

Tutte sono formate da cartoncini, o lastrine metalliche, aventi una quadrettatura saltuariamente

forata in modo che il crittogramma si ricava dalla scrittura del testo chiaro nei successivi fori della griglia.

Le *griglie quadrate*, inventate da Cardano nel XVI secolo, possono avere il lato di un numero qualsiasi di quadretti; per cifrare si usa soltanto un quarto dei quadretti (escluso quello centrale nei quadrati a numero dispari di caselle), perchè la griglia si usa in quattro posizioni facendola ruotare successivamente di 90° su un foglio sottostante di carta quadrettata avente le stesse dimensioni, per modo che vengono a risultare successivamente scoperti i quadretti del foglio, nei quali si scrivono le lettere del testo chiaro. Si rileva indi il crittogramma in uno dei modi visti.

Per corrispondere in cifra a mezzo delle griglie quadrate occorre che sia stabilita la posizione iniziale della griglia. Per decifrare basta scrivere il crittogramma ricévuto su un foglio quadrettato delle dimensioni della griglia, sovrapporvi la griglia nelle quattro successive posizioni leggendo senz'altro il testo chiaro.

Per costruire una griglia quadrata si procede così: stabilito il lato del quadrato, si quadretta la placca di cartone o metallo, quindi si fora a caso un quadretto e poi si determinano i quadretti che verranno ad assumere la posizione simmetrica a quella del quadretto scelto nelle tre successive rotazioni della griglia, questi quadretti non dovranno più essere forati; si sceglie un secondo quadretto e si procede in modo analogo, si continua collo stesso metodo fino ad avere forato un quarto dei quadretti

della placca (escluso sempre quello centrale quando esista).

Nella figura 1 è dato un esempio di cifratura con griglia quadrata di sei caselle per lato, nella quale il testo chiaro: «Nostra offerta rifiutata riducete prezzo» rilevato per colonne dalla sinistra dà il crittogramma:

E A R A Z = D N E T A = I I T E R = Z I U O P = T R O F T = T A O F C = S R E R F = U

Le griglie indefinite ideate dal Sacco sono placche rettangolari quadrettate aventi un numero stabilito di righe orizzontali ed un numero indefinito di colonne verticali (numero colonne variabile e numero linee costante); ciascuna colonna ha un numero fisso di fori scelti completamente a caso.

Per cifrare si scrive il testo chiaro per colonna, adoperando tutti i fori delle successive colonne fino ad averlo scritto tutto; poi si rileva il crittogramma per linee, formandone dei gruppi di tante lettere quanti sono i fori esistenti in ciascuna colonna.

Per decifrare si divide il numero delle lettere del crittogramma pel numero dei fori contenuti in ciascuna colonna e così si conosce il numero delle colonne da impiegare; si scrive poscia il crittogramma per linea, arrestandosi al numero della colonna ricavato dalla precedente divisione.

Il crittogramma si legge poi facilmente per colonna.

Una griglia indefinita può essere quella rappresentata nella fig. 2.

A
B
C
D
1ª
N O S
T
R
A O
F
F
2ª
N O S
E T R
R T
A A O R
I F F
I F U
3ª
N T O S
A E T R
T R T A
A A R O R
I I F F
D I U F C U
4ª
E N T O T S
A E E P T R
R T R T A E
A A Z R O R
Z I I O F F
D I U F C U

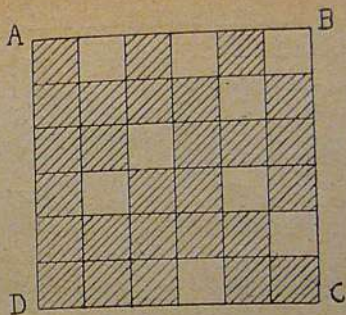
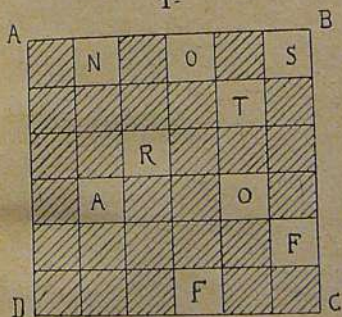
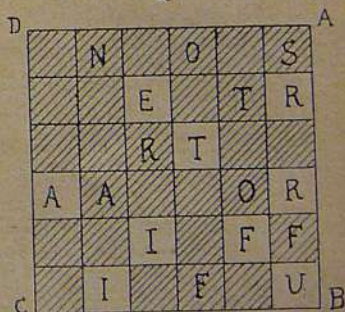
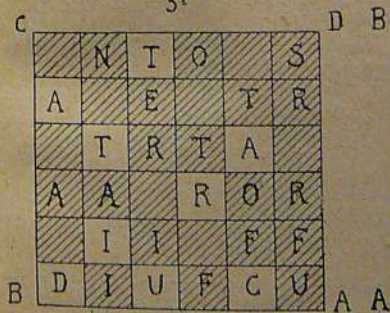
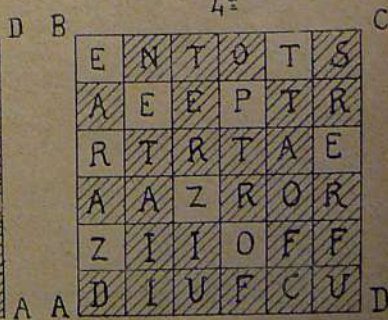



Fig. 1.

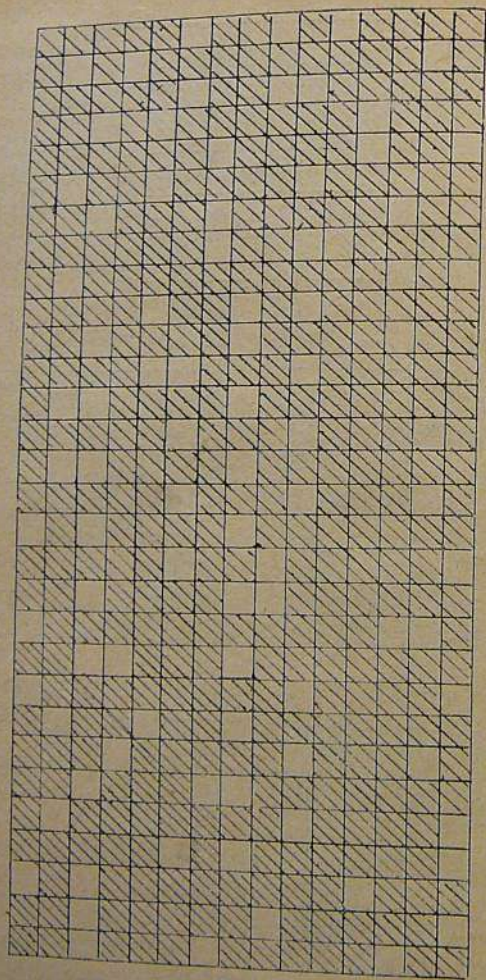



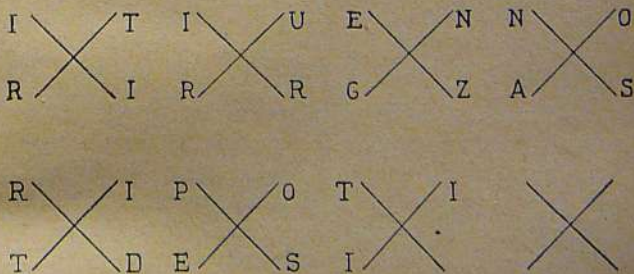
Fig. 2.

Le griglie hanno l'inconveniente, come mezzo di cifratura, di comportare l'esistenza di un documento che può essere perduto, trafugato o copiato.

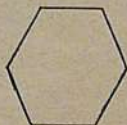
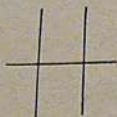
Trasposizione con figure.

Per la corrispondenza tra poche persone è di una certa praticità il sistema di utilizzare, come guida per la trasposizione, delle figure geometriche; bisogna però ben stabilire quante figure si debbano impiegare in ogni linea orizzontale, da quale punto si debba iniziare la scrittura del testo chiaro e quale ordine si debba seguire.

Si debba cifrare per esempio:

« Ritiri urgenza nostri depositi »

rilevando per orizzontali si otterrà il crittogramma:

ITIVE = NNORI = RRGZA = SRIPO = TITDE = SI

Si possono usare anche altre figure:

III. — *Sistemi letterali di cifratura a sostituzione.*

Generalità.

Nei sistemi a sostituzione le lettere del testo chiaro vengono sostituite con altre lettere, oppure con numeri od anche con altri segni qualunque. Però per la corrispondenza telegrafica sono usati soltanto i sistemi che impiegano gruppi omogenei di lettere, o di numeri, per le ragioni viste.

La cifratura con questi sistemi si effettua servendosi per la sostituzione di uno solo o di più alfabeti cifranti, nel primo caso il sistema è detto *monoalfabetico*, nel secondo *polialfabetico*.

Nei sistemi *monoalfabetici* si impiegano quindi

soltanto due liste alfabetiche: una costituita dalle 26 lettere dell'alfabeto della lingua ed eventualmente dai primi 10 numeri cardinali, nel loro ordine alfabetico naturale; l'altra, detta alfabeto cifrante, comprendente altrettanti segni quanti la prima, ciascuno dei quali corrisponde ad uno della lista chiara.

Nei sistemi polialfabetici invece, mentre l'alfabeto chiaro rimane sempre unico, gli alfabeti cifranti, possono essere moltisssimi e vengono usati alternativamente secondo l'indicazione data da una chiave.

Vedremo il modo di preparare gli alfabeti cifranti e di impiegare le chiavi.

Facciamo rilevare subito come quando si abbia un alfabeto chiaro comprendente più di 26 segni oppure quando si usino alfabeti cifranti formati con numeri, non sia possibile sostituire ogni segno dell'alfabeto chiaro con una sola lettera, o numero, o segno dell'alfabeto cifrante, ma occorra adoperarne almeno due. Da ciò deriva che i testi cifrati risultano più lunghi dei testi chiari.

Modi di formare gli alfabeti cifranti.

I sistemi a sostituzione sono generalmente usati senza l'impiego di documenti, il che è un vantaggio per la segretezza, occorre quindi conoscere vari modi di formare gli alfabeti cifranti, mediante regole semplici da potersi tenere facilmente a memoria; ne esporremo qualcuno cominciando dai più semplici.

1.° Si sposta l'alfabeto normale di un certo numero di posti:

Chiaro: A B C . . . . M N O . . . . Z
Cifrante: N O P . . . . Y Z A . . . . M

2.° Si rovescia e si sposta l'alfabeto normale di alcuni posti:

Chiaro: A B C . . . . L M N O . . . . Y Z
Cifrante: N M L . . . . C B A Z . . . . P O

3.° Si ricava l'alfabeto cifrante mediante una trasposizione con chiave:

C	A	V	O	R	E	T	T	O
2	1	9	4	6	3	7	8	5
A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	

Alfabeto cifrante:
B K T A J S F O X D M V I R
E N W G P Y H Q Z C L U

4.° Si ricava l'alfabeto cifrante con una trasposizione con chiave, scrivendo però l'alfabeto chiaro sotto la chiave cominciando successivamente ogni riga orizzontale in corrispondenza delle successive colonne 1, 2, 3, ecc.

L'alfabeto cifrante poi, anzichè essere rilevato nell'ordine indicato dalla chiave numerica, può esserlo dalla destra o dalla sinistra, o per diagonali.

B	A	R	L	E	T	T	A
3	1	6	5	4	7	8	2
=	A	B	C	D	E	F	G
=	=	=	=	=	=	=	H
I	J	K	L	M	N	O	P
=	=	=	=	Q	R	S	T
=	=	=	U	V	W	X	Y
=	=	Z	=	=	=	=	=

Alfabeto cifrante rilevato per colonna dalla sinistra:

I A J B K Z C L U D M Q V E N R
W F O S X G H P T Y

5.º Si ricava l'alfabeto cifrante da una chiave mnemonica, la quale si scrive in una riga toglendone le lettere che in essa eventualmente si ripetono; sotto si scrivono le restanti lettere dell'alfabeto normale, indi si rileva in uno dei noti modi:

chiave: PREPOTENZA

P R E O T N Z A	Alfabeto cifrante rilevato
B C D F G H I J	per colonna da sinistra:
K L M Q S U V W	A J W Z I V N H U T G S O F Q E
X Y	D M R C L Y P B K X

6.º Per ottenere maggiore complicazione gli alfabeti cifranti possono ricavarsi compiendo successivamente due delle operazioni indicate ai numeri precedenti.

Gli alfabeti cifranti così ricavati si dispongono poi in corrispondenza dell'alfabeto chiaro e si ottiene così la lista cifrante, che nell'uso potrebbe servire anche come lista decifrante, ma per comodità nel decifrare si può preparare una lista nella quale si mette in ordine alfabetico l'alfabeto cifrante ed in corrispondenza si mettono le lettere equivalenti dell'alfabeto chiaro.

Sostituzione monoalfabetica semplice.

Convenuto quale sia l'alfabeto cifrante la cifratura e la decifratura con questo sistema sono molto facili.

Supponiamo di avere ricavato l'alfabeto cifrante

nel modo 3° e di esserci preparata questa lista cifrante :

Chiaro: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Cifrante: B K T A J S F O X D M V I R E N W G P Y H Q Z C L U

Se abbiamo da cifrare il seguente testo chiaro:

« Agitazione personale cresce venite subito »

basterà cercare in corrispondenza di ciascuna delle sue lettere, presa nell'alfabeto chiaro, l'equivalente lettera presa nell'alfabeto cifrante e scrivere senz'altro il crittogramma per gruppi di cinque lettere:

B F X Y B = U X E R J = N J G P E = R B V J T =
G J P T J = Q J R X Y = J P H K X = Y E

Per decifrare si cerca nell'alfabeto chiaro la corrispondente di ogni lettera del crittogramma, presa nell'alfabeto cifrante.

Questo sistema presenta pochissime garanzie di sicurezza, si è quindi cercato di renderlo più complesso.

Sostituzione monoalfabetica con nulle ed omofoni.

Come vedremo trattando della decrittazione, uno degli elementi per iniziarla è il computo delle frequenze delle lettere (o dei numeri) che esistono nei crittogrammi ed il confronto con le frequenze caratteristiche delle varie lettere nel linguaggio normale. — Per eliminare perciò tale elemento di debolezza si è pensato di introdurre nei sistemi monoalfabetici dei segni senza significato corrispondente, detti *nulle*, e di usarne parecchi in corri-

spondenza delle lettere più frequentemente usate nel linguaggio normale, questi sono detti *omofoni*.

Naturalmente l'introduzione di nulle e di omofoni nell'alfabeto cifrante richiede l'impiego di un numero di segni maggiore di quello dell'alfabeto chiaro.

Per far ciò si possono combinare a due a due i primi dieci numeri cardinali (0,1, 2......9) ottenendo 100 gruppi cifranti; od anche combinare a due a due le 26 lettere dell'alfabeto ottenendo 676 gruppi. Volendo disporre di maggior numero di gruppi cifranti si possono usare le combinazioni a tre a tre, a quattro a quattro, ecc.

Per compilare la lista cifrante si stabilisce quante nulle si vogliono usare, quanti gruppi si vogliono far corrispondere a ciascuna lettera dell'alfabeto, a ciascun numero, a ciascun segno di punteggiatura, ecc., tenendo conto della diversa frequenza di ciascuno di essi.

Quindi si estraggono a sorte i gruppi da far corrispondere all'alfabeto chiaro, onde avere una corrispondenza assolutamente irregolare, per non fornire nessun appiglio ai decrittatori, che presto scoprirebbero, se esistesse, una qualsiasi regola di corrispondenza tra chiaro e cifrante.

Una tabella, costituita coi 100 gruppi ottenuti colle combinazioni dei 10 primi numeri due a due, per cifrare col sistema a sostituzione monoalfabetica con nulle ed omofoni, è la seguente compilata mediante sorteggio.

A 36-33 25-11 97-94	F 74-72	M 89-53	S 70-15	Y 85	Nulle 32-81 16-78 27-65 08-39 52-88 34-41 80-30 40-77 14-38	Uno 56-01	Sei 23
B 87-84	G 54-46	N 69-48	T 37-17	Z 19-83		Due 20	Sette 09
C 76-62	H 43-99	O 71-50 58-35 63-42	U 67-10 29-13 59			Tre 51	Otto 31
D 49-44	I 04-73 02-86 98-68	P 57-24	V 90-26			Quattro 95	Nove 21
E 05-00 93-79 66-61	J 91	Q 60-28	W 96			Cinque 12-47	Zero 92
	K 75	R 55-22 07	X 45			Punto 18-03	Virgola 06
	L 82-64						

Si debba cifrare con questa tabella il testo chiaro:
« Sciopero dichiarato carboni aumentano »
si otterrà, impiegando nulle ed omofoni il seguente testo cifrato:

15. 76. 68. 78. 50. 24. 79. 55. 39. 71. 49. 41. 02. 62. 99. 86. 38. 33. 22. 11. 17. 58. 80. 62. 97. 55. 08. 87. 63. 69. 27. 04. 25. 13. 32. 53. 00. 48. 37. 94. 48. 16. 71. 52. 08

che si trasmetterà scrivendolo per gruppi di cinque cifre così: 15766 = 87850 = 24795 = 53971 49410 = 26299 = ecc. ecc.

Nel cifrare le nulle e gli omofoni vanno impiegati con abilità saltuariamente.

Per decifrare si divide il crittogramma ricevuto in gruppi di due numeri e se ne cerca il significato in una tabella decifrante, che converrà prepararsi disponendo i gruppi numerici in ordine progressivo e scrivendovi accanto il significato chiaro.

Sostituzione polialfabetica.

Questo sistema di cifratura è stato ideato da G. B. Porta di Napoli verso la metà del sec. XVI; successivamente venne modificato dal Vigenère in Francia, da Tritemio in Germania e da altri senza però mutarne il principio fondamentale.

Assai usato fino a pochi anni fa nella corrispondenza diplomatica ed in quella militare, conserva ancora oggi il suo valore perchè il più idoneo ad essere applicato nelle macchine per cifrare (vedi cap. V) ed è probabile che acquisti ancora notevole importanza.

È basato sul principio di impiegare 26 liste cifranti, diverse l'una dall'altra, individuata ciascuna da una lettera dell'alfabeto o da un numero; le liste cifranti vengono adoperate per cifrare ciascuna lettera del testo chiaro secondo l'ordine indicato dalle lettere di una chiave. La chiave, di varia lunghezza (parola, frase, numero, successione incoerente di lettere o di numeri), concordata fra i corrispondenti, viene scritta lettera per lettera sotto le successive lettere del testo chiaro, allo scopo

ab	A	B	C	D	E	F	G	H	I	J	K	L	M
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
cd	A	B	C	D	E	F	G	H	I	J	K	L	M
	Z	N	O	P	Q	R	S	T	U	V	W	X	Y
ef	A	B	C	D	E	F	G	H	I	J	K	L	M
	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
gh	A	B	C	D	E	F	G	H	I	J	K	L	M
	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
ij	A	B	C	D	E	F	G	H	I	J	K	L	M
	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
kl	A	B	C	D	E	F	G	H	I	J	K	L	M
	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
mn	A	B	C	D	E	F	G	H	I	J	K	L	M
	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
op	A	B	C	D	E	F	G	H	I	J	K	L	M
	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
qr	A	B	C	D	E	F	G	H	I	J	K	L	M
	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
st	A	B	C	D	E	F	G	H	I	J	K	L	M
	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
uv	A	B	C	D	E	F	G	H	I	J	K	L	M
	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
wx	A	B	C	D	E	F	G	H	I	J	K	L	M
	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
yz	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	N

Fig. 3.

predetto di indicare l'alfabeto da impiegare per la cifratura di queste ultime.

Vedremo ora alcuni tipi di questo sistema.

Sistema del Porta. — La tavola originale del Porta si vede nella figura 3, essa comprende soltanto 13 alfabeti cifranti, nei quali la prima riga è sempre eguale e la seconda varia pel semplice spostamento di un posto a destra.

Per cifrare quindi, colla chiave indicata nella colonna a sinistra, una lettera della prima metà dell'alfabeto la si cercherà nella prima riga e la si sostituirà con quella sottostante; per cifrare una lettera della seconda metà la si cercherà nella riga inferiore e si sostituirà con la corrispondente della riga superiore. Per decifrare si procede in modo perfettamente simile.

Vogliamo ad esempio cifrare colla tavola del Porta e con la chiave: TORINO

testo chiaro:	Q U E S T A	N O T T E
chiave:	T O R I N O	T O R I N
testo cifrato:	M B W J M T	J I B K Y

Sistema del Vigenère. — Nella figura 4 è riprodotta la tavola completa del Vigenère, la quale consta di 26 alfabeti, dei quali il 1º è un alfabeto normale e gli altri sono successivamente derivati collo spostamento semplice di una lettera dalla coda alla testa; ciascun alfabeto è individuato dalla sua prima lettera a sinistra. Per comodità si sono aggiunti in alto un alfabeto, dove si cerca la lettera

da cifrare o da decifrare; a sinistra un alfabeto dove si cerca la lettera chiave quando si cifra; a destra un alfabeto rovesciato (meno la 1ª lettera) dove si cerca la lettera chiave quando si decifra.

CHIAVE PER CIFRARE

CHIARO	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	CIFRATO
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	Z
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	Y
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	X
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	W
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	V
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	U
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	T
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	S
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	R
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	E	G	H	I	J	Q
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	P
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	O
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	E	G	H	I	J	K	L	M	N
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	E	G	H	I	J	K	L	M	N	M
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	L
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	J
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	I
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	H
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	G
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	F
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	E
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	D
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	C
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Z	B

CHIAVE PER DECIFRARE

Fig. 4.

Per cifrare si cerca nell'orizzontale superiore la lettera del chiaro, nella verticale a sinistra la lettera chiave, all'incrocio delle due linee si trova la lettera cifrata. Per decifrare si cerca nell'orizzontale superiore la lettera cifrata; nella verticale a destra la lettera chiave, all'incrocio delle due linee si trova

la lettera chiara. Vediamo un esempio pratico di cifratura con questa tavola:

testo chiaro: S O S P E N D E T E   C O M P E R E
chiave: C R E M O N A C R E   M O N A C R E
testo cifrato: U F W B S A D G K I   O C Z P G I I

Complicazioni dei sistemi polialfabetici.

Come si è detto i sistemi polialfabetici originali furono molto usati, ma quando vennero diffusi i metodi per la loro decrittazione si cercò di renderli maggiormente segreti. Due provvedimenti essenziali furono per ciò adottati: l'uso di alfabeti più complicati e non derivati l'uno dall'altro con regole così semplici; l'impiego di chiavi di ciframento molto lunghe.

Il primo provvedimento può essere attuato in una infinità di modi, ed il lettore potrà sbizzarrirsi quanto vorrà, bisogna però tener presente che conviene ricavare il primo ed i successivi alfabeti con una regola mnemonica semplice, allo scopo di non avere bisogno di conservare documenti, sempre pericolosi pel mantenimento del segreto.

Per quanto invece riguarda la ricerca di chiavi molto lunghe esporremo alcuni modi di ottenerle, avvertendo anche in questo caso che regole se ne possono trovare molte, purchè siano sempre mnemoniche.

1.° usare come chiave lunghe frasi o brani di libri, facilmente ritenibili a memoria o che usualmente si hanno a portata di mano. — Si corre però

il rischio che chi insidia il nostro segreto appena scoperto una parte della chiave possa ricostruire facilmente il resto;

2.° stabilire una chiave mnemonica breve mediante la quale si esegue una volta o due la trasposizione (vedi n. II, cap. IV) di parecchi alfabeti normali ripetuti; si possono ottenere in tal modo serie lunghissime di lettere incoerenti da adoperare come chiave di ciframento;

3.° si stabilisce una chiave mnemonica breve e la si trasforma in chiave numerica, poi come chiave di ciframento si impiega la serie costituita dei vari pezzi della prima chiave presi arrestandosi successivamente ai numeri 1, 2, 3, ecc. della chiave numerica. Un esempio pratico chiarirà meglio l'idea:

Chiave mnemonica: P O R D E N O N E
Chiave numerica: 8 6 9 1 2 4 7 5 3

Chiave di ciframento da usare:

P O R D P O R D E P O R D E N O N E P O R D E N P O R D E N O N P O P O R D E N O P P O R

Un altro modo di evitare che la chiave, o quanto meno la sua lunghezza, possa venire scoperta, a causa della regolarità con cui si ripetono gli alfabeti cifranti usando chiavi corte, è quello di interrompere arbitrariamente ogni tanto la chiave.

Per raggiungere tale intento si può operare così: dalla tavola di sostituzione polialfabetica si elimina una delle lettere di raro uso, per es. la W o la K (sostituibili caso mai con due V o con C H, ri-

spettivamente), la tavola risulterà così soltanto di 25 alfabeti; si sceglie quindi una lettera come indicatrice dell'interruzione di chiave, tra quelle frequentemente usate nel linguaggio ordinario, per es. P; nella tavola di ciframento si elimina la P dappertutto e la si sostituisce con la W (o la K). In tal modo chi riceve il crittogramma quando in esso incontra la P è avvertito che deve interrompere la chiave e che alla P non corrisponde alcuna lettera del testo chiaro.

Supponiamo di dover cifrare con la tavola del Vigenère, con la convenzione ora fatta e con chiave RONCHI il testo

chiaro:	T R O	V A T O A	G E	N T E
chiave interrotta:	R O N	R O N C H	R O	R O N
crittogramma:	K F B P	M O G Q H P	X S P	E K R

Per far scomparire la regolarità prodotta da una chiave breve si possono anche usare i metodi di *autociframento:* col testo chiaro o col testo cifrato.

In entrambi i casi si impiega una chiave mnemonica breve per cifrare le prime lettere del testo chiaro, quindi la cifratura si prosegue impiegando come lettere della chiave o le lettere stesse del testo chiaro, o le lettere del testo cifrato che man mano si ottengono, si ha così praticamente una chiave di lunghezza indefinita.

Se dovessimo cifrare un testo chiaro nei modi predetti, valendosi della chiave ausiliaria RAVENNA, l'operazione si presenterebbe così:

1.º Autocifreamento col chiaro:

chiaro: RIUNIONE DOMANI SOLITO POSTO
chiave: RAVENNAR IUNION EDOMAN ISOLI

crittogramma: (si può ricavare con qualunque tabella polialfabetica):

2.º Autocifreamento col cifrato:

chiaro: RIUNIONE DOMANI SOLITO POSTO
chiave: RAVENNAM VECPHA YTDYTD VEKXW
crittogr: MVECPHAY TDYTDV EKXWCC ecc.

Questo modo, che in sostanza è un allungamento di chiave, è lento e richiede molta attenzione nelle operazioni di cifratura e decifratura.

Sostituzione di gruppi di lettere con altrettanti gruppi di egual numero di lettere.

Come è stato detto al capitolo III la cifratura per sostituzione, oltrechè su ogni singola lettera, si può effettuare su gruppi di lettere; cioè si può eseguire la cifratura per poligrammi, come comunemente si dice.

L'operazione si può fare sostituendo gruppi di 2, 3, 4 lettere del testo chiaro con altrettanti gruppi cifranti di egual numero di lettere.

Questo tipo di sostituzione si può effettuare in diverse maniere.

Per predisporre i gruppi del testo chiaro:

1.º si possono raggruppare le lettere 2 a 2, 3 a 3, nell'ordine in cui è compilato;

2.º si può scriverlo in 2, 3 ecc. righe sovrapposte, a pezzi di 3, 4, 5, 6, 7 lettere per ciascuna riga e continuando il testo nella riga successiva; poi si prosegue il testo stesso in un altro blocchetto di righe, e così di seguito fino alla fine; questa operazione preparatoria si dice seriare per 3, per 4, ecc.

Per esempio il testo chiaro «Comunichi prezzi odierni» si può preparare così: CO = MU = NI = = CH = IP = RE = ZZ = IO = DI = ER = NI, oppure seriando per quattro:

C O M U = I P R E = D I E R
N I C H = Z Z I O = N I X X

i gruppi da cifrare saranno: CN = OI = MC = UH = IZ = PZ . . . . . . EX = RX.

Nel caso restino posti vuoti in una riga si completano con lettere incoerenti.

Per eseguire la sostituzione:

a) si può preparare una lista contenente le combinazioni delle lettere dell'alfabeto prese due a due, tre a tre, ecc. alle quali se ne fanno corrispondere altrettante di egual numero di lettere; ma il sistema è incomodo perchè richiede l'esistenza di un documento;

b) si impiegano tabelle a doppia entrata, od anche combinazioni di n numeri presi n ad n (che si possono facilmente preparare con regole mnemoniche).

Per dare un'idea di questi sistemi ne esporremo uno di sostituzione di gruppi di due lettere (bigrammi) che fu impiegato dall'Esercito Inglese du-

rante la guerra mondiale, col nome di *Playfair cipher*.

Coll'aiuto di una chiave mnemonica si costruisce una tabellina quadrata di 25 lettere che serve per cifrare i bigrammi; la tabella essendo di 25 lettere, invece di 26, bisogna scartarne una, che in italiano può essere la W.

Per costruire la tabella si prepara un quadrato di 25 caselle, in esse si scrivono le lettere della chiave senza ripetere quelle già scritte (vedi modo 5º di formare gli alfabeti cifranti) e poi le restanti lettere dell'alfabeto regolare.

Per cifrare si seguono le seguenti norme:

1.º le lettere chiare che si trovano in una stessa colonna si cifrano con le lettere che stanno loro sotto (l'ultima della colonna colla prima);

2.º le lettere chiare che sono sulla stessa riga si cifrano con quelle che sono alla loro destra (l'ultima a destra colla prima a sinistra);

3.º le lettere chiare che sono su linee e colonne diverse si cifrano con quelle che fanno rettangolo con esse, cominciando da quella che è la 1ª nel bigramma chiaro;

4.º se il bigramma chiaro è composto da due lettere eguali si cerca di eliminare il fatto inserendo una lettera di raro uso.

Il testo chiaro si può preparare in uno dei modi visti. Vediamo un'applicazione pratica di questo sistema; sia la chiave mnemonica COSTANTINOPOLI, il testo da cifrare: « Spedite subito munizioni », che si preparerà seriato per cinque. Le operazioni da compiere sono le seguenti:

1.º Preparare la tabella

C	O	S	T	A
N	I	P	L	B
D	E	F	G	H
J	K	M	Q	R
U	V	X	Y	Z

2.º Seriare il testo chiaro per cinque:

S P E D I   I T O M U   N
T E S U B   N I Z I O   I

3.º Cifrarlo bigramma per bigramma:

chiari: ST=PE=ES=DU=IB=IN=TI=OZ=MI=UO=NI
cifrati: TA=IF=FO=JC=PN=PI=OL=AV=KP=VC=IP

4.º Trasmetterlo a gruppi di 5 lettere:

T A I F F = O J C P N = P I O L A = V K P V C = I P

Per decifrare si compiono in ordine inverso tutte le operazioni fatte per cifrare.

Sostituzione di lettere con frazionamento.

Questo tipo di cifratura si dice a frazionamento perchè ogni lettera del testo chiaro viene prima sostituita con due o più lettere, numeri o segni, questi vengono poi nuovamente cifrati per sostituzione o per trasposizione, di guisa che i vari elementi cifranti di una sola lettera chiara risultano frazionati e mescolati nel crittogramma.

I sistemi usati si possono raggruppare intorno a tre tipi:

1.° si sostituiscono dapprima le lettere del chiaro coi segni dell'alfabeto Morse, questi poi si cifrano per sostituzione;

2.° si cifrano prima le lettere del chiaro per sostituzione con gruppi di due o tre lettere o cifre, che poi si cifrano a loro volta per trasposizione;

3.° si cifrano prima per sostituzione le lettere del chiaro con gruppi di due (o tre) cifre, che si traspongono e poi ancora si cifrano nuovamente sostituendole per gruppi di due (o tre) cifre con una sola lettera.

Il 1° ed il 2° tipo rendono il crittogramma più lungo del testo chiaro, il 3° tipo lo conserva di eguale lunghezza.

Daremo alcuni esempi dei vari tipi.

1° tipo: *Sistema Pollux.* — Ciascuna lettera del testo chiaro viene prima sostituita colla equivalente nell'alfabeto Morse e separata dalla successiva con uno spazio; a ciascun segno dell'alfabeto Morse

(punto •, linea —, spazio +) si fanno corrispondere più numeri scelti nella serie 0, 1, 2 . . . . . 9 come una piccola lista monoalfabetica con omofoni: si cifra ciascuno dei segni Morse nella prima sostituzione effettuata con uno dei numeri equivalenti; effettuata questa 2ª sostituzione si traspone in uno dei modi noti e finalmente si trasmette il crittogramma rilevato da questa per gruppi di 5 numeri.

Sia da cifrare RITIRARE; le operazioni da fare saranno le seguenti:

1.º preparare la lista cifrante dei segni Morse:

punto (·) = 4, 1, 7, 0
linea (-) = 3, 2, 6
spazio (+) = 5, 8, 9

2.º sostituire alle lettere chiare le equivalenti nell'alfabeto Morse e sostituire ai segni Morse i numeri corrispondenti

```
 R       I     T     I       R       A       R     E
· — · + · · + — + · · + · — · + · — + · — · + · +
4 6 0 9 1 7 5 3 9 4 0 8 7 2 1 5 4 6 8 0 3 4 9 7 9
```

3.º effettuare su quest'ultima serie numerica la trasposizione semplice (o con chiave)

```
4 6 0 9 1 7
5 3 9 4 0 8
7 2 1 5 4 6
8 0 3 4 9 7
9
```

4.º rilevarla, per es., per colonne dalla destra, e compilare senz'altro il crittogramma definitivo per gruppi di 5 numeri: 78671 = 04994 = 54091 = 36320 = 45789.

Per decifrare si compiono le stesse operazioni, ma in senso inverso.

Questo sistema può essere reso più complicato e più segreto adoperando le lettere invece dei numeri per preparare la lista cifrante dei segni Morse, si dispone così di un maggior numero di omofoni.

2º tipo: *Sistema Collon.* — Le lettere del testo chiaro vengono singolarmente cifrate con bigrammi presi in una tabella quadrata di 25 lettere (del tipo visto nel Playfair cipher), il bigramma è dato dalle coordinate della lettera chiara, scegliendo l'origine in uno qualunque dei quattro vertici.

I bigrammi cifranti si scrivono in colonna sotto la corrispondente lettera chiara e quindi si rilevano, seriandoli per 4, per 5 o per 6, e si trasmettono al solito per gruppi di 5 lettere.

Le successive operazioni da fare per cifrare il testo chiaro ACQUISTATE, con la chiave mnemonica VILLANOVA saranno:

1.º preparare la tabella quadrata (escludendo la W):

V	I	L	A	N
O	B	C	D	E
F	G	H	J	K
N	P	Q	R	S
T	U	X	Y	Z

2.° cifrare il testo chiaro coi bigrammi cifranti sottoposti, prendendo come origine delle coordinate il vertice inferiore sinistro e leggendo prima l'ascissa e poi l'ordinata; seriare questi, per es., per 4:

A C Q U   I S T A   T E

{ Y X X U ^ U Z T Y ^ T Z
{ V O N T   V N T V   T O

3.° rilevare e trasmettere il crittogramma (per gruppi di 5 lettere)

Y X X U V = O N T U Z = T Y V N T = V T Z T O

Per decifrare si fanno le identiche operazioni in ordine inverso.

Questo sistema può essere complicato in vari modi; usando una chiave mnemonico-numerica di

10 lettere e quindi 10 numeri che si possono adoperare come coordinate esterne alla tabella, secondo una regola mnemonica qualunque convenuta e ricavata dalla chiave; il crittogramma definitivo sarà così formato da numeri anzichè da lettere.

I tedeschi durante la guerra mondiale usarono un sistema di cifratura di questo tipo, con coordinate esterne in lettere, il quale era reso più solido facendo subire una trasposizione con chiave al 1º crittogramma ottenuto con la tabella.

3º tipo: *Sistemi Delastelle*. — Il crittologo Delastelle ha immaginato molti sistemi di cifratura; qui di seguito ne esporremo due, da lui denominati *bifido* e *trifido*.

Per cifrare col sistema detto *bifido* si impiega una tabella della stessa forma di quella vista nel sistema Collon, con coordinate esterne individuate da numeri stabiliti d'accordo fra i corrispondenti; indi si cifra una prima volta il testo chiaro con questa tabella scrivendo i bigrammi sovrapposti; questi bigrammi vengono poi rilevati seriando per 3, per 4, ecc.; la serie di numeri così ottenuta si cifra per gruppi di due numeri una seconda volta valendosi della primitiva tabella, colla quale da ogni coppia di numeri, presi uno sull'orizzontale e l'altro sulla verticale, si ricava la lettera che trovasi all'incrocio di queste due linee. Finalmente le lettere così ricavate costituiscono il crittogramma definitivo, che si trasmette, come di solito, per gruppi di 5 numeri.

Renderemo più evidenti con un esempio le successive operazioni da compiere.

Si debba cifrare il testo chiaro COMPRATE, usando la chiave mnemonica VILLAGLORI per la preparazione della tabella di 25 lettere (esclusa la W):

1.º si preparerà la tabella quadrata, nella quale si conviene di leggere prima il numero sulla verticale e poi quello sull'orizzontale:

	1	2	3	4	5
1	V	I	L	A	G
2	O	R	B	C	D
3	E	F	H	J	K
4	M	N	P	Q	S
5	T	U	X	Y	Z

2.º si cifra il testo chiaro con la tabella, scrivendo i bigrammi sovrapposti:

```
C O M P R   A T E
2 2 4 4 2 ^ 1 5 3
4 1 1 3 2   4 1 1
```

3.° si rilevano i bigrammi cifranti seriati per 5 e si cifrano a loro volta colla tabella usata inversamente:

22	44	24	11	32	15	34	11
R	Q	C	V	F	G	J	V

4.° il crittogramma definitivo da trasmettere sarà:

R Q C V F = G J V

Il sistema *trifido* comprende una serie di operazioni che per maggior semplicità e chiarezza indicheremo valendoci di un esempio pratico:

a) Si prepara un alfabeto cifrante di 27 lettere, impiegando anche la *e* accentata (È), in uno dei modi già visti (n. III del capitolo IV), e noi qui useremo una trasposizione con chiave di 9 lettere:

T	E	L	E	G	R	A	F	O
9	2	6	3	5	8	1	4	7
A	B	C	D	E	È	F	G	H
I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z

b) si rileva l'alfabeto per colonna (nell'ordine dato dalla chiave numerica) e si scrivono in colonna sotto ciascuna lettera le 27 combinazioni dei numeri 1, 2, 3 presi tre a tre:

F	O	X	B	J	S	D	L	U	G	P	Y	E	M	V	C	K	T	H	Q	Z	È	N	W	A	I	R
1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3	3	3
1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3	1	1	1	2	2	2	3	3	3
1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3	1	2	3

c) con questa tabella si cifra il testo chiaro, scrivendo i trigrammi (gruppi di tre numeri) cifranti in colonna sotto la corrispondente lettera del chiaro:

P	A	R	T	E	D	O	M	A	N	I	S	E	R	A
2	3	3	2	2	1	1	2	3	3	3	1	2	3	3
1	3	3	3	2	3	1	2	3	2	3	2	2	3	3
2	1	3	3	1	1	2	2	1	2	2	3	1	3	1

d) si rilevano i trigrammi cifranti seriandoli per esempio per 5 e si cifra la serie così ottenuta (a gruppi di tre numeri) valendosi della tabella di cui alla lettera *b*) usata in senso inverso:

233	221	333	221	331	112	333	123	212
T	E	R	E	A	O	R	S	P

212	312	333	223	323	131
P	Q	R	V	W	D

e) la serie di lettere così ricavata costituisce il crittogramma da trasmettere, nel modo ripetuto:

TEREA = ORSPP = QRVWD

Questo secondo sistema Delastelle è alquanto complicato, ma dà dei crittogrammi realmente difficili da decrittare.

Per decifrare i crittogrammi compilati con uno dei due sistemi il destinatario eseguirà tutte le operazioni già viste per cifrare, ma in senso inverso.

IV. — *Doppia cifratura coi sistemi letterali.*

Una seconda cifratura coi sistemi letterali aumenta la segretezza, non in tutti i casi però, ed è da adottarsi quando sia veramente necessario tale aumento e lo si ottenga realmente; essa richiede maggior tempo per cifrare e per decifrare e aumenta la probabilità di commettere errori. Tutti i sistemi letterali di trasposizione e di sostituzione possono essere applicati abbinati, ma non tutti danno un rendimento effettivo ai fini del rinforzo del segreto.

Così dicasi di due successive trasposizioni con chiave o di una doppia sostituzione monoalfabetica.

Danno buoni risultati invece le combinazioni di una sostituzione e di una trasposizione con chiave, specialmente quando la sostituzione sia polialfabetica e sia fatta seguire alla operazione di trasposizione.

Anche una trasposizione seguita da una sostituzione a gruppi di lettere (sono sufficienti i bigrammi) dà buona solidità alla cifratura.

Il lettore che ha fin qui seguito l'esposizione dei metodi crittografici letterali potrà praticamente provare e trovare varie combinazioni convenienti.

CAPITOLO V.

GLI APPARECCHI E LE MACCHINE PER CIFRARE

Allo scopo di assicurare sempre una maggiore segretezza alle operazioni di cifratura gli studiosi di crittografia si sono dedicati alla ricerca di congegni meccanici che consentissero di cifrare e di decifrare senza l'uso di tabella, o di oggetti come la griglia, o di qualsiasi altro documento facile ad essere trafugato, copiato o perduto, od anche permettessero di operare automaticamente con chiavi numerose e molto lunghe, che come abbiamo visto danno massima sicurezza.

Le ricerche si sono rivolte ai sistemi letterali di trasposizione e di sostituzione che in genere si prestano ad essere applicati con mezzi meccanici, ed un numero grande di tali mezzi è stato proposto; questi li possiamo distinguere in *apparecchi per cifrare* se di piccola mole, portatili e relativamente semplici; ed in *macchine per cifrare* se di struttura tale da non poter essere portati indosso alla persona ed anzi da dover essere comunemente impiegati installati in un ufficio.

Gli apparecchi e le macchine hanno l'inconveniente di esistere materialmente, quindi di doversi avere sempre a portata quando occorra cifrare e decifrare, mentre i sistemi mnemonici non richiedono la presenza di cosa alcuna salvo al momento di eseguire le operazioni crittografiche.

È fuori di dubbio che la rapidità e la sicurezza di impiego delle macchine per cifrare ne renderanno estesa la diffusione presso le grandi organizzazioni politiche e commerciali.

I. — *Apparecchi per cifrare.*

Le trasposizioni semplici o con chiave e le sostituzioni mono o polialfabetiche si possono eseguire meccanicamente con apparecchi semplici, taluni anche rudimentali, che possono costruirsi facilmente o che si trovano in commercio.

Essendo ormai noti al lettore i principî di costituzione e d'impiego dei sistemi letterali ci limiteremo a dare un cenno di alcuni apparecchi in uso.

Apparecchio Bazeries (fig. 5). — È costituito da un rocchetto sul quale si infilano 20 anelli metallici, che hanno ciascuno inciso sull'orlo esterno un diverso alfabeto trasposto di 25 lettere; ogni anello ha inoltre un numero ed una lettera per individuarlo.

La chiave viene formata servendosi dei numeri, o delle lettere, caratteristici di ogni anello, e quindi può essere numerica o letterale della lunghezza di 20 lettere o numeri; essa viene composta di volta

in volta secondo l'ordine col quale si infilano gli anelli sull'asse.

Per cifrare, dopo messi a posto gli anelli sull'asse secondo l'ordine indicato dalla chiave, basta far girare gli anelli successivamente in modo da comporre lungo una generatrice le prime venti lettere del testo chiaro; sulle altre 25 generatrici risultano delle serie incoerenti di lettere, una qualunque di queste serie si potrà prendere come testo cifrato;

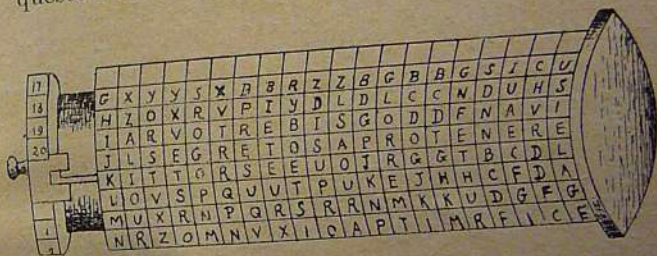



Fig. 5.

si ripete poi l'operazione a pezzi di 20 lettere fino ad aver cifrato tutto il testo chiaro.

Per decifrare si procede in modo perfettamente identico: si infilano gli anelli nell'ordine dato dalla chiave; si fanno risultare su una generatrice le prime venti lettere del crittogramma: girando tutto l'apparecchio apparirà su un'altra generatrice il testo chiaro.

L'apparecchio è geniale, ma si è constatato che possedendolo si può per tentativi riuscire a decrittare i crittogrammi, di cui si sia venuti in possesso, cifrati con l'apparecchio stesso.

Cifrario universale a regolo (fig. 6). — È costituito, come appare dalla figura, da un telaio metallico, di cm. 16×10, nel quale scorrono orizzontalmente

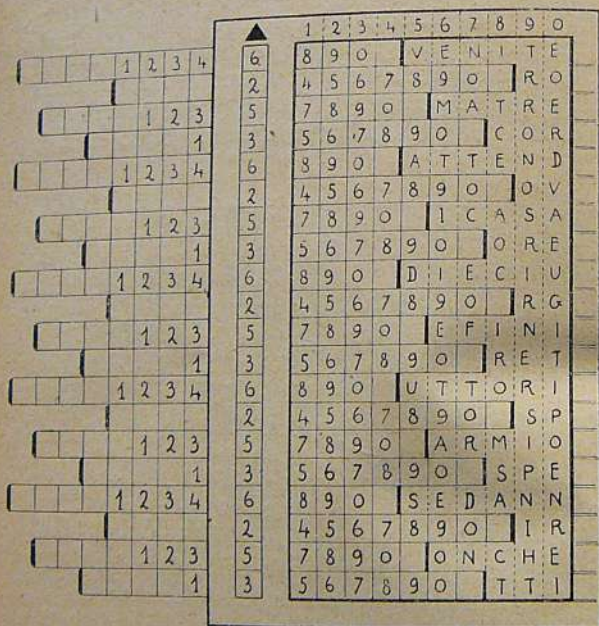



Fig. 6.

venti regoli portanti ciascuno una numerazione da 1 a 20.

Estraendo i vari regoli in modo da combinare nella finestrella verticale (sormontata dal trian-

golo) una chiave numerica, che può essere fino di venti numeri, si vengono a scoprire nel corpo del telaio le sottostanti caselle di un foglio quadrettato, nelle quali si scriverà per linea (o per colonna) il testo chiaro e quindi si potrà rilevarlo per colonna (o per linea), od in altro qualsiasi ordine, purchè sia diverso da quello nel quale è stato scritto il testo chiaro; si spedirà poi a gruppi di 5 lettere. Se il testo chiaro contiene un numero di lettere superiore al numero delle caselle che risultano scoperte dopo composta la chiave, si ripete l'operazione tante volte quante occorre, collo stesso procedimento.

L'apparecchio, pur presentando l'inconveniente comune a tutti gli apparecchi: cioè quello di esistere, ha buone qualità di segretezza, specialmente quando la società che ne ha preso il brevetto (Roma, — Via Mortaro, 19) vi avrà apportato alcune modificazioni, intervertendo la numerazione dei venti regoli, che attualmente è uguale per tutti e in ordine regolare, come appare dalla figura.

Le operazioni da eseguire per decifrare sono evidenti esaminando la struttura dell'apparecchio.

Apparecchio Ducros o Scotografo (fig. 7). — È simile al Bazeries, se ne differenzia però perchè è formato da 13 anelli metallici con incisi sul bordo 13 alfabeti regolari di sole 20 lettere (sono escluse Q, J, W, X, Y); sopra il cilindro costituito dagli anelli si infila un collare mobile composto di 5 anelli, portanti sul bordo incisi i numeri da 1 a 9 ed aventi una finestrella, tra questa ed i numeri è lasciato l'intervallo di un posto. Con i 5 anelli si può for-

mare un numero di 5 cifre e di conseguenza sul collare risulteranno le 5 finestrelle disposte in varia maniera, gli anelli del collare si serrano con un dispositivo in modo che non si muovano durante tutta l'operazione.

Per cifrare si dispongono gli anelli del rocchetto nell'ordine indicato da una chiave mnemonica let-

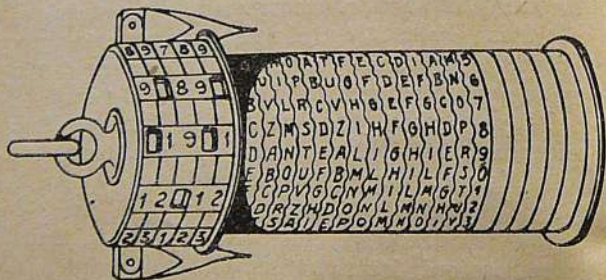



Fig. 7.

terale e gli anelli del collare secondo l'ordine dato da una chiave numerica; si fa poi scorrere il collare fino a leggere attraverso la finestrella del 1º anello la 1ª lettera del chiaro, quindi la 1ª lettera del cifrato si leggerà attraverso la finestrella del 2º anello del collare; poi si legge la 2ª lettera del chiaro attraverso la finestrella del 2º anello e la 2ª lettera del cifrato attraverso la finestrella del 3º anello, così si continua fino ad avere cifrato la 5ª lettera. Si sposta poi di un posto il collare e si ripete l'operazione per gruppi di 5 lettere fino ad avere cifrato tutto il testo chiaro.

L'apparecchio, che in conclusione dà una cifratura polialfabetica con chiave di 65 lettere, non dà però sufficiente garanzia di segreto.

Regoli e cerchi per cifrare. — Gli apparecchi più semplici, ideati già fin dal XVI secolo dal Porta, per cifrare coi sistemi a sostituzione sono costituiti da due regoli o da due cerchi concentrici scorrevoli o girevoli l'uno rispetto all'altro; su ciascun regolo o cerchio è segnato un alfabeto regolare oppure trasposto; uno degli alfabeti si adopera come chiaro e l'altro come cifrante, secondo una convenzione fatta tra i corrispondenti.

Non consideriamo il caso, in cui sulle due parti siano segnati due alfabeti regolari, ed il cifrante sia spostato di un certo numero di posti rispetto al chiaro perchè questo equivarrebbe ad una sostituzione monoalfabetica semplice, di cui abbiamo visto la assoluta inefficacia.

Consideriamo invece il caso di avere su uno dei regoli l'alfabeto regolare e sull'altro un alfabeto trasposto in uno dei modi noti, si potrà così effettuare la sostituzione polialfabetica con chiave di qualunque lunghezza, limitata soltanto dall'abilità del cifratore nel non commettere errori.

Abbiamo visto che nella sostituzione polialfabetica si impiegano tre lettere: la chiave, la chiara, la cifrata.

Adoperando i regoli ovviamente le lettere vengono ad affacciarsi due a due, bisogna quindi assumere una quarta lettera colle funzioni di *indice*, che può essere scelta ad arbitrio.

Il Sacco ha compiuto esaurienti studi sui regoli cifranti e con l'abituale acutezza ha ricavato le regole di costruzione e d'impiego che qui di seguito sono riassunte.

Queste geniali deduzioni non erano mai state fatte nel passato da altri ed hanno creato la possibilità di valersi di questi semplici apparecchi, facilmente costruibili, con una garanzia di segreto che può essere sufficiente in parecchi casi.

alfabeto regolare	U V W X Y Z A B C D E F G H I J K L M N O P Q R S T

alfabeto trasposto	M A H Q O B Y I S Z N C J U T D V E F K W R G P X L

Variando sui regoli la posizione relativa delle quattro lettere: indice, chiave, chiara, cifrata, si ottengono con una stessa chiave 12 crittogrammi differenti per uno stesso testo chiaro.

Questa affermazione si può facilmente verificare: si deve però far osservare che, tra i 12 modi di cifrare così ottenibili, due soli danno una considerevole garanzia di segretezza, cioè quelli risultanti dagli schemi seguenti:

1.º	alfabeto regolare:	indice	chiave
	alfabeto trasposto:	chiara	cifra
2.º	alfabeto regolare:	indice	chiave
	alfabeto trasposto:	cifra	chiara

perchè gli altri 10 modi equivalgono a tabelle polialfabetiche in cui gli alfabeti sono molto semplicemente derivati gli uni dagli altri, mentre coi due modi indicati la derivazione è molto complessa e difficilmente rilevabile. L'impiego di questi regoli dà buoni risultati quando le chiavi e gli alfabeti intervertiti siano variati con frequenza.

Per cifrare col regolo, supponendo di aver stabilito la convenzione di cui allo schema 1°, si fa scorrere uno dei listelli fino a far coincidere la lettera chiara colla lettera indice e poi si legge in corrispondenza della lettera chiave la lettera cifrata.

Per decifrare: si porta la lettera cifrata a coincidere colla lettera chiave ed in corrispondenza della lettera indice si legge la lettera chiara.

Col regolo costruito come nello schema riprodotto supposto G la lettera indice ed N la lettera chiave, la lettera chiara J sarebbe cifrata con la lettera K.

II. — *Macchine per cifrare.*

Si è visto come la resistenza dei sistemi di sostituzione polialfabetici si possa aumentare coll'impiego di chiavi molto lunghe, ma il cifrare con chiavi molto lunghe impone grandissima attenzione da parte dei cifratori ed è causa di errori con conseguenze gravi: il saltare una lettera della chiave rende il crittogramma indecifrabile. — Si è per ciò cercato di costruire delle macchine che diano automaticamente chiavi di ciframento di grandissima lunghezza, ripromettendosi da esse diversi van-

taggi, anzitutto la maggior resistenza dei crittogrammi alla decrittazione; l'eliminazione di quasi tutte le cause d'errore, avendosi anche macchine che scrivono direttamente il crittogramma; la maggiore rapidità nel cifrare e nel decifrare ed una conseguente economia di personale.

V'ha però il rovescio della medaglia: le macchine sono di costo elevato, sono ancora delicate e perciò in uffici di grande importanza occorre disporre anche di una riserva, non potendosi ammettere una interruzione nelle operazioni crittografiche; inoltre, come si è già accennato, non tutte sono facilmente trasportabili.

Tuttavia, dati i vantaggi ed i miglioramenti che saranno realizzati, si può ritenere che il loro impiego si diffonderà sempre più, specialmente nei Ministeri, nelle grandi Banche e nelle Società che gestiscono impianti radiotelegrafici.

Trattandosi di un argomento che ha un'importanza pel suo sviluppo avvenire, riteniamo opportuno diffonderci alquanto circa i principî sui quali sono fondate e costruite queste macchine.

Uno degli elementi su cui si fonda la decrittazione dei sistemi polialfabetici è la ricerca della lettera, o delle lettere, più frequenti, che ovviamente in ogni alfabeto cifrante saranno sempre sostituite dalla stessa lettera; scoperte quindi le lettere più frequenti nei vari alfabeti si risale facilmente al loro significato chiaro. È noto che gli alfabeti cifranti sono individuati ciascuno da una lettera della chiave.

Ora siccome è necessario nella decrittazione cer-

care di scoprire la lunghezza della chiave, ci si basa sul fatto che se la chiave è di n lettere avremo che la 1ª, la n + 1, la 2 n + 1 lettera del crittogramma saranno cifrate collo stesso alfabeto cifrante, ed analogamente la 2ª, la n + 2, la 2 n + 2, ecc.; cioè se n è piccolo avremo in breve raccolto buon numero di lettere-cifra derivanti da identici alfabeti cifranti e quindi potremo facilmente scoprire quale sia la lettera più frequente in ciascuno di quei dati alfabeti.

Se invece n è grande si comprende facilmente che può darsi che nel crittogramma non vi siano 2 n + 1 lettere ed allora la ricerca della lettera più frequente diventa più ardua, perchè per la ricerca non si dispone che della 1ª e della n + 1 lettera (presentandosi le altre una volta sola), e può darsi che nessuna di queste sia la più frequente.

Le considerazioni precedenti dimostrano quanto avevamo affermato al capitolo IV circa la convenienza delle chiavi lunghe e spiegano come nelle macchine da cifrare si cerchi di fare in modo che gli alfabeti cifranti vengano impiegati in un modo complicato, eliminando qualsiasi regolare periodicità e facendo in modo che una serie di lettere chiave non si ripeta nello stesso ordine che dopo un intervallo lunghissimo.

Di macchine dove è applicato questo principio ne sono state costruite diversi tipi: in Germania la « Enigma », in Inghilterra dalla Patent Developping C.ie, in Svezia dalla Aktiebolaget Cryptograph di Stoccolma; alcune usano chiavi lunghe con alfabeti trasposti, altre chiavi lunghissime con alfa-

beti regolari; queste ultime sono preferibili perchè non è necessario tenere segreta la macchina. Le macchine sono sovente accoppiate ad apparecchi scriventi, sì che battendo il testo chiaro appare automaticamente il cifrato e viceversa.

Schematicamente possono raffigurarsi così: dalla tastiera di una macchina speciale partono tanti conduttori elettrici quante sono le lettere che si possono battere, i fili vanno a corrispondere ad altrettante spine poste sulla periferia di un quadrante circolare fisso. — L'abbassamento di un tasto provoca il passaggio di una corrente elettrica che produce lo spostamento della corrispondente spina.

Di fronte al quadrante fisso esiste un quadrante analogo sul quale sono ricavati tanti contatti quante sono le spine del primo quadrante, a tali contatti fanno capo altrettanti fili che vanno a collegarsi con le leve della macchina stampante.

Battendo un tasto della tastiera speciale si produce così lo spostamento di una spina del primo quadrante che va a toccare un contatto del 2º quadrante e che perciò provocherà il passaggio di una corrente nel filo collegato con quel contatto, la corrente determinerà la stampa della lettera collegata alla leva corrispondente.

Se si fa in modo che il secondo quadrante, pur mantenendo i suoi vari contatti periferici sempre collegati con le stesse leve della macchina stampante, possa ruotare affacciando i proprî contatti di fronte alle diverse spine del 1º quadrante e se si stabilisce inoltre che gli spostamenti successivi del secondo quadrante avvengano ad ogni battuta con

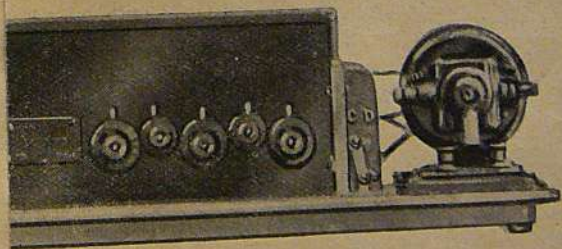
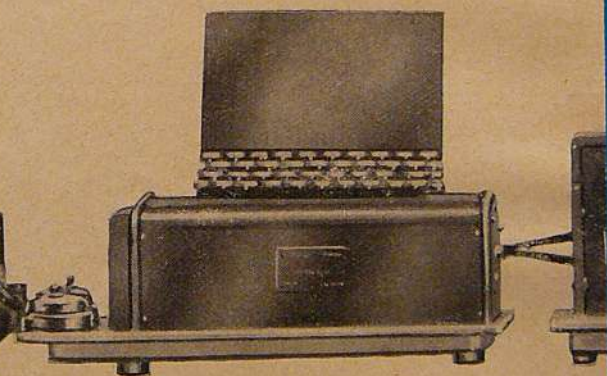
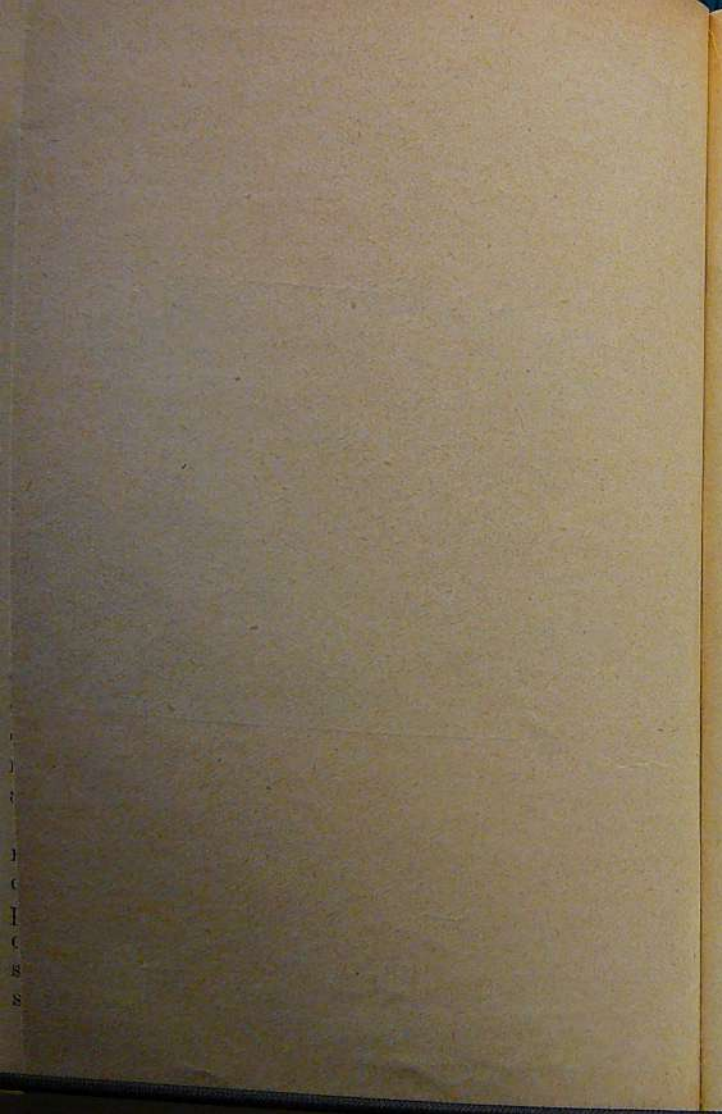



Fig. 8. — Macchina per cifrare.

ampiezza sempre diversa, senza derivare da una combinazione semplice e non avente una qualsiasi periodicità, si avrà la meccanica applicazione di una chiave di ciframento al testo chiaro battuto sulla tastiera speciale.

Le combinazioni delle posizioni relative dei due quadranti permettono di ottenere periodi di milioni di lettere prima che due tratti di chiaro siano cifrati identicamente.

Dispositivi particolari consentono di compiere analogamente le operazioni di deciframento.

Nella figura 8 si vede un tipo di macchina per cifrare della casa A. B. Cryptograph di Stoccolma (Drottninggatau 6). La macchina dà automaticamente il testo cifrato su una macchina da scrivere o, in caso di trasmissione telegrafica, su una perforatrice; serve tanto per cifrare, quanto per decifrare. Le chiavi possono essere indicate da parole scelte ad arbitrio da ritenersi a memoria.

La macchina si compone di una tastiera speciale, dell'apparecchio crittografico propriamente detto e di una macchina da scrivere, o di una perforatrice, secondo i casi.

Per cifrare: il testo chiaro viene battuto sulla tastiera speciale (la centrale della figura) e la macchina da scrivere o la perforatrice, da il crittogramma in gruppi di 5 lettere, anche se il chiaro contiene altri segni. — Per decifrare: il crittogramma viene battuto sulla tastiera speciale e il testo chiaro appare sulla macchina da scrivere.

Con questa macchina il periodo di ciframento è di 67.830 lettere, quindi oltrepassa di massima la lunghezza dei più lunghi testi chiari.

Le varie combinazioni di chiavi sono ottenute mediante la chiusura arbitraria di contatti elettrici nell'apparecchio crittografico (parte di destra della figura); questi contatti sono in numero di 57, quindi è evidente che la combinazione delle chiavi può essere variata quasi all'infinito. I contatti si possono disimpegnare in un secondo e l'apparecchio si chiude con un catenaccio. È inoltre possibile disporre tanto l'apparecchio crittografico quanto la macchina da scrivere in diversi ambienti, allo scopo di porre il testo cifrato o decifrato al riparo dalla vista della persona che batte, il chiaro o il crittogramma, sulla tastiera speciale.

La stessa casa ha costruito anche una macchina portatile. In sintesi si può dire che queste macchine danno una considerevole garanzia di segretezza.

CAPITOLO VI.

I SISTEMI DI CIFRATURA A REPERTORIO

Caratteristiche generali.

I sistemi di cifratura a repertorio, come si è detto al capitolo III, applicano anch'essi il procedimento della sostituzione, ma a differenza dei sistemi letterali l'operazione anzichè su lettere, o su gruppi di poche lettere o su frazioni di lettera, si eseguisce su sillabe, parole, frasi, numeri, ed anche su lettere.

Mentre per cifrare coi sistemi letterali ci si basa fondamentalmente su regole mnemoniche, colle quali si preparano di volta in volta i documenti per le operazioni crittografiche, con quelli a repertorio ci si serve di documenti anche voluminosi preventivamente compilati e distribuiti ai vari corrispondenti che devono usarli.

Tali documenti, detti codici, repertori, cifrari, dizionari per corrispondenza in cifra, sono sinteticamente costituiti da liste di varia lunghezza nelle quali a ciascun elemento chiaro corrisponde un gruppo cifrante.

Di liste ve ne possono essere una o due.

Se ne ha una quando agli elementi chiari disposti in ordine alfabetico regolare corrispondono i gruppi cifranti pure disposti in ordine regolare, e basta appunto una lista perchè tanto per cifrare quanto per decifrare la ricerca degli elementi chiari, o di quelli cifrati, è resa agevole dalla regolare elencazione di entrambi. Il tipo ad una sola lista è detto codice regolare ed è poco resistente. Sono invece necessarie due liste, quando agli elementi chiari disposti in ordine alfabetico corrispondono dei gruppi cifranti scelti senza alcuna regolarità di successione, quindi, mentre per cifrare si procederebbe con facilità, altrettanto non avverrebbe per decifrare, poichè si dovrebbero rintracciare faticosamente i gruppi cifrati. Perciò si usa una seconda lista nella quale vengono disposti in un ordine regolare di successione i gruppi cifrati ed in corrispondenza si pongono gli elementi chiari equivalenti, che a loro volta risulteranno in questa lista in ordine incoerente. — La 1ª lista (o fascicolo, o volume) è detta cifrante, la 2ª è detta decifrante.

I codici sono di impiego molto comodo perchè si possono compilare con quel numero di elementi chiari che si vuole, tale numero dipende dal tipo di corrispondenza che si deve cifrare, inoltre danno il vantaggio di poter cifrare anche intere frasi con un solo gruppo cifrante, con risparmio di tempo e di denaro.

I gruppi cifranti sono costituiti con un numero di lettere o di cifre variabile da 2 a 5 come massimo, perchè, come è noto, in base alle convenzioni

telegrafiche internazionali ciascun gruppo di cifre conta per tante parole quante volte contiene cinque cifre, più una parola per l'eventuale eccedenza.

Il numero di gruppi cifranti da introdurre nel codice deriva dal numero degli elementi chiari fissati, più gli omofoni e le nulle.

A seconda dei segni impiegati per formare i gruppi cifranti se ne possono combinare le seguenti quantità massime:

con gruppi di 2 lettere	$26^2 = 676$
con gruppi di 2 numeri semplici	$10^2 = 100$
con gruppi di 3 lettere	$26^3 = 17576$
con gruppi di 3 numeri	$10^3 = 1000$
= = = = = = = = = = = = = = = = = =	
= = = = = = = = = = = = = = = = = =	
con gruppi di 5 lettere	$26^5 = 11.881.376$
con gruppi di 5 numeri	$10^5 = 100.000$

Naturalmente le lettere ed i numeri possono essere impiegati solo in parte ed allora il numero dei gruppi cifranti ottenibili è minore; la loro quantità si può facilmente ricavare coi procedimenti del calcolo combinatorio.

Del tipo regolare si trovano in commercio codici detti paginati nei quali i gruppi cifranti risultano dalla riunione di un numero di 2 o 3 cifre, scritto in testa a ciascuna pagina, con un altro gruppo di 2 o 3 cifre scritto a lato dell'elemento chiaro.

Le pagine sono numerate progressivamente, in ordine diretto od inverso, ma saltuariamente; questa numerazione può essere variata a piacere e

d'intesa fra i corrispondenti e costituisce il fattore di segretezza del codice. In ciascuna pagina vi sono generalmente 100 gruppi invariabili e che possono essere in ordine regolare od anche incoerente, data la minore difficoltà di rintracciarli nella decifrazione nel limitato campo di una pagina. Sono poco consigliabili perchè danno scarse garanzie di segretezza.

Circa la struttura dei codici intervertiti abbiamo già detto, in essi nel volume cifrante gli elementi chiari sono disposti come in un vocabolario ed accanto a ciascuno è scritto l'intero gruppo cifrante; nel volume decifrante si può in taluni casi avere una disposizione analoga a quella dei codici paginati, cioè il gruppo cifrato spezzato in due parti: una in testa alla pagina ed una in ciascuna riga con a fianco il corrispondente significato chiaro dell'intero gruppo.

Sembra opportuno far rilevare come i codici, pur tanto comodi e pratici, abbiano una grave difetto dal lato del segreto, cioè l'assoluta esigenza di essere custoditi gelosamente.

Compilazione dei codici.

I codici che danno realmente qualche garanzia di custodire il segreto sono quelli intervertiti, come chiaro risulta dall'esame della loro struttura.

Vediamo perciò particolarmente come si possa procedere alla compilazione di questi.

Come si è accennato, la loro mole dipende dalla natura delle corrispondenze alle quali sono destinati, è quindi su di queste che bisogna studiare prima di costruire il codice, poichè è anche risaputo che ogni arte, professione o mestiere, usa nelle relazioni quotidiane un linguaggio proprio limitato ad un certo numero di parole e di frasi abitudinarie, e tra queste parole alcune sono usate più frequentemente ed altre meno. — Si è inoltre osservato che il personale addetto alla cifra acquista particolari abitudini.

Da queste osservazioni e dalla considerazione che sono i testi cifrati quelli che possono più facilmente cadere in possesso degli interessati a svelarne il contenuto, deriva la opportunità di compiere le ricerche appunto sui crittogrammi trasmessi dall'ente cui deve servire il codice in un recente periodo di tempo; non disponendo di crittogrammi si può anche lavorare su testi chiari.

Da questo esame appariranno le parole e le frasi impiegate più di frequente e le abitudini dei cifratori; si ricaveranno così gli elementi per stabilire la mole del cifrario, le necessità di omofoni e la loro misura, le frasi e le espressioni che conviene cifrare con un solo gruppo e relativi omofoni. Si completa poi il codice con molti gruppi nulli, con tutti gli elementi della punteggiatura, le desinenze delle coniugazioni, le sillabazioni che possono servire per formare parole non contenute nel codice, ecc.

Formato così con cura la lista cifrante, e stabiliti in conseguenza quanti gruppi cifranti occor-

rono, si fissa di quante cifre (o lettere) deve essere formato ciascuno di questi, quindi si estraggono completamente a sorte i successivi gruppi cifranti che devono corrispondere agli elementi chiari (compresi omofoni e nulle).

L'operazione del sorteggio è della massima importanza, perchè in generale nessun sistema di cifratura, ed in particolare i codici, deve presentare la benchè minima simmetria e regolarità di costruzione, di modo che i decrittatori non possano scoprire alcuna regola che una volta trovata fornisca molti elementi in una volta sola. Così il sorteggio dei gruppi cifranti nei codici non permette di trarre alcuna deduzione sul significato di un gruppo quando si sia per avventura scoperto quello del gruppo vicino; questo evidentemente non si può evitare nei codici paginati, ed in ciò consiste la loro debolezza.

Per costruire la lista decifrante si dispongono in successione regolare i gruppi cifrati che sono stati impiegati nella lista cifrante e ad essi si fanno corrispondere gli elementi chiari. Questa in sostanza è un'operazione secondaria che si deve eseguire per la necessità di consentire la ricerca rapida dei gruppi per la decifrazione.

A titolo di curiosità diamo qui l'elenco dei codici di cifratura che si trovano in commercio:

Autore	Titolo	Lingua	a gruppi di	comprend. gruppi
Airenti . . .	*Diction. chiffré*	francese	5 cifre	59.200
Baravelli. . .	*Dizionario*	italiano	4 cifre	10.000
Bazeries . . .	*Tables ciffrantes et dechif.*	francese	4 cifre	10.000
Bolton. . . .	*Diction. chiffré*	inglese	lettere	
Brachet . . .	*Diction. chiffré*	francese	5 cifre	10.000
Brunswick . .	*Diction. pour la correspondance télégrafique secrète*	francese	4 cifre	10.000
Darhan . .	*Clave telegrafica*	spagnolo	5 cifre	32.400
Katscher . .	*Wörterbuch*	tedesco	4 lettere	
Krohn . . .	*Buchstaben für die Chiffrirung ecc.*	tedesco	lettere	
Louis	*Diction. pour la corr. secrète*	francese	5 cifre	20.000
Mamert-Gallian	*Diction. telegrafique economique et secr.*	francese	3 lettere	17.576
Mengarini . .	*Nuovo cifrario*	italiano	5 cifre	
Niethe. . . .	*Wörterbuch*	tedesco	5 cifre	27.446
Nilac	*Diction. chiffré*	francese	4 cifre	10.000
Sittler . . .	*Dict. abréviatif chiffré*	francese	4 cifre	10.000
Slater. . . .	*Code*	inglese	5 cifre	25.000
Stern e Steiner	*Chiffrierbuch*	tedesco	4 cifre	10.000
Walter. . . .	*Dechiffrier Wörterbuch*	tedesco	lettere	

Seconda cifratura dei codici.

Abbiamo visto che usando codici intervertiti costruiti razionalmente si ottiene già una grande comodità d'impiego e una buona garanzia di segreto. Ma quando si voglia avere una fortissima sicurezza non ci si può contentare di una semplice cifratura e fa d'uopo ricorrere ad una seconda cifratura, detta anche sopracifratura.

Questa ha lo scopo di far sparire la forma abituale dei gruppi cifranti e la loro ripetizione nella identica forma, così da rendere infruttuoso il raffronto che potesse esserne fatto, da chi ne avesse l'interesse, tra un testo chiaro ed il corrispondente testo cifrato.

È chiaro che tutti i sistemi letterali, di cui si è trattato, potrebbero essere adoperati per una seconda cifratura dei codici, ma non tutti danno un vantaggio reale e praticamente i migliori risultati si ottengono con alcuni pochi sistemi e più precisamente:

la trasposizione semplice o con chiave;
la sostituzione letterale mono o polialfabetica;
le sostituzioni a poligrammi.

Vediamo quindi come si possa effettuare la seconda cifratura coi detti sistemi.

La trasposizione semplice o con chiave, che si compie nel modo esposto al capitolo IV; è già un buonissimo mezzo, ma è molto laboriosa specialmente quando si tratti di operare su crittogrammi

lunghi, con essa la fisonomia normale dei gruppi cifranti effettivamente scompare.

La sostituzione letterale mono o polialfabetica viene eseguita su ogni cifra del chiaro mediante una o più liste (alfabeti o serie di numeri) di sostituzione. Impiegando una lista sola l'operazione è semplice, ma meno sicura; impiegando più liste naturalmente occorre l'ausilio di una chiave, che viene convenuta tra i corrispondenti, oppure indicata nel crittogramma mediante un gruppo cifrante indicatore, che evidentemente se la chiave si cambia più volte nel crittogramma deve essere cifrato con la chiave precedente; il primo gruppo successivo al gruppo indicatore sarà quindi cifrato con la nuova chiave.

Un procedimento analogo a questo è quello delle chiavi aggiuntive o sottrattive, che consistono in un gruppo di cifre, generalmente in numero disuguale da quello dei gruppi cifranti. che si aggiungono o sottraggono, cifra per cifra, a quelle del 1º crittogramma senza mai eseguire riporti.

Per esempio se si deve sopracifrare un 1º crittogramma a gruppi di 5 cifre con la chiave aggiuntiva 5147 si farà così:

1º crittogramma:	36174	82865	14172	65912
chiave aggiuntiva:	51475	14751	47514	75147
2ª cifratura:	87549	96516	51686	30059

La sopracifratura mediante sostituzione a poligrammi è uno dei sistemi più usati, si applica mediante tabelle o liste cifranti, nelle quali i gruppi

di due o tre cifre vengono sostituti con altrettanti gruppi di eguale numero di cifre.

Le liste o tabelle, come si è ripetutamente avvertito, devono essere preparate senza alcuna regolarità, il sorteggio sarà sempre il miglior metodo da seguire. Esse saranno costruite in modo diverso a seconda che i gruppi ricavati dalla 1ª cifratura sono di 3, 4 o 5 cifre; se sono di 4 cifre basterà una unica lista o tabella contenente 100 gruppi di 2 cifre coi quali si sostituiranno i successivi bigrammi contenuti nel 1º crittogramma.

Se invece i gruppi cifranti sono di 3 o 5 cifre si possono usare:

liste di sostituzione monoalfabetica per una cifra e liste di bigrammi per le altre coppie di cifre;

oppure liste di bigrammi e liste di trigrammi da usare successivamente per ogni gruppo;

od anche soltanto liste di bigrammi o soltanto liste di trigrammi, facendo un nuovo raggruppamento per 2 o per 3 cifre dei numeri contenuti nel 1º crittogramma.

In altri termini il seguente crittogramma, ottenuto dopo una 1ª cifratura:

90487 = 68485 = 22231 = 31744

può essere così preparato per la sopracifratura:

9=04=87=6=84=85=2=22=31=3=17=44;
90=487=68=485=22=231=31=744;
904=87=684=85=222=31=317=44;
90=48=76=84=85=22=23=13=17=44;
904=876=848=522=231=317=44.

Il crittogramma sopracifrato definitivo poi dovrà essere trasmesso a gruppi di 5 cifre.

La sopracifratura per sostituzione a poligrammi si può fare nel modo detto a parole pronunciabili, che ha l'unico scopo di evitare errori di trasmissione.

Ne facciamo cenno perchè qualche codice in commercio ne fa uso. Tale metodo sfrutta il fatto che le convenzioni telegrafiche internazionali tassano per una sola parola i gruppi cifrati contenenti fino a 10 lettere se sono parole pronunziabili.

Perciò si è pensato di sostituire i bigrammi od i trigrammi della 1ª cifratura con parole di 4 o 5 lettere, che quindi riuniti, per sopracifrare anche un gruppo di 5 lettere, danno una parola di 8 o 10 lettere. Basandosi su questo criterio si possono combinare liste e tabelle svariatissime, tenendo ancora presente che s'intendono per parole pronunciabili non soltanto quelle aventi un significato reale nella lingua corrente, ma anche quelle del tipo, ad esempio come: *citumefepo*, *sobasirugi*, e simili.

Le tabelle di sopracifratura presentano gli stessi pericoli dei codici, insiti nella loro materiale esistenza, di più la prudenza consiglia di disporne di parecchie: Quindi per avere una vera garanzia di segreto occorre custodirle con ogni cura, cambiarle spesso e adoperarne diverse per uno stesso crittogramma, avvisando in questo caso il destinatario del cambiamento di tabella mediante gruppi indicatori, con le modalità che abbiamo più sopra esposto.

CAPITOLO VII.

LA DECRITTAZIONE

I — *Considerazioni generali.*

La decrittazione è l'operazione, anzi la laboriosa serie di operazioni, con cui si tende a tradurre in chiaro un crittogramma senza conoscere le regole o possedere i documenti crittografici ad esso relativi.

Premettiamo senz'altro che non si possono stabilire regole tassative e generali per la decrittazione di tutti i sistemi.

La decrittazione è un lavoro generalmente molto difficile e che richiede in chi vi si applica numerose qualità spiccate: in primo luogo una profonda conoscenza ed una lunga pratica dei sistemi crittografici in genere e dei procedimenti di decrittazione in particolare, ed inoltre doti di costanza e di pazienza, acuto spirito d'osservazione, uniti ad un particolare intuito, che, come in tutte le arti, è dono naturale di pochi privilegiati.

Con questo non si vuole affermare che insormon-

tabili difficoltà esistano per divenire buon decrittatore, ma si vuol far rilevare come non tutti possano diventarlo, essendo difficile trovare tante qualità riunite in una sola persona ed ove si rifletta ancora che l'ottimo decrittatore deve necessariamente conoscere diverse lingue e possibilmente alcuni dialetti.

Dobbiamo però considerare che in pratica di decrittatori non ne occorre un gran numero, e quindi è facile trovare tra gli appassionati di quest'arte il numero occorrente; ed anche si deve por mente che di solito non si tratta di operare su uno solo o su pochi crittogrammi tecnicamente perfetti, ma all'opposto si lavora su numerosi documenti ben soventi compilati senza soverchia cura.

Ma chi voglia giovarsi razionalmente della crittografia deve pur sempre pensare che pochi decrittatori abili sono capaci di un altissimo rendimento e rappresentano un'insidia da non trascurare; deve quindi adoperarsi perchè i procedimenti di cifratura siano sempre scelti tra i più sicuri ed applicati con ogni cautela.

Abbiamo detto che non esistono regole generali per la decrittazione, ne esistono però di particolari per i principali sistemi conosciuti, ma soprattutto esiste un metodo di lavoro, metodo comune a tutte le scienze sperimentali; si tratta cioè di osservare e analizzare gli elementi disponibili per gettare le basi di una ipotesi, formulare l'ipotesi, tentarne la verifica esperimentando la fondatezza, scartarla se non risponde, ma se risponde all'esperienza perseguirla con tenacia fino ad aver raggiunto lo scopo.

Non è a dirsi però che questo lavoro conduca sempre a risultati positivi, talvolta questi non si raggiungono o si raggiungono quando non sono più fruttiferi.

Anche nel campo della decrittazione il Sacco ha compiuto studi di una sorprendente acutezza ed ha trovato ed esposto metodi che nessun crittologo aveva mai intuito. La sua estesa conoscenza dei sistemi di cifratura e la sua profonda coltura matematica gli hanno consentito di scoprire nuovi metodi che hanno condotto a risultati inimmaginabili.

I vari principî che ora verremo esponendo sono in massima parte frutto degli studi del Sacco; studi che per essere interamente e chiaramente esposti richiederebbero da soli un ponderoso volume.

Quanto tuttavia si trova in questo Manuale è sufficiente per orientare la mente del lettore in questa branca dell'arte crittografica.

II. — *Procedimenti generali di decrittazione.*

Quando si debba decrittare, le principali operazioni da compiere sono: la ricerca della lingua d'origine, la ricerca del sistema di cifratura usato, la ricostruzione del testo chiaro e della chiave (regola o cifrario).

La ricerca della lingua d'origine di solito non presenta difficoltà, perchè quasi sempre si conosce la provenienza del crittogramma, o se non si conosce si compiranno indagini per rintracciarla.

Il ricercare il sistema di cifratura presenta già una relativa difficoltà, ma, come vedremo in seguito, la conoscenza della struttura dei vari sistemi è di forte aiuto, ed inoltre occorre effettuare la statistica delle lettere o dei numeri esistenti nel crittogramma ricavandone la frequenza assoluta e quella percentuale; la stessa statistica si esegue per le ripetizioni di bigrammi, trigrammi eguali ed in particolar modo, in alcuni casi, per le lettere a sequenze obbligate. Vedremo in seguito l'importanza del computo delle frequenze e delle sequenze.

La ricostruzione del testo chiaro e della chiave usata si effettua specialmente con accorgimenti particolari per ogni sistema, dei quali daremo un cenno, tuttavia si possono enunciare alcuni modi di operare comuni a parecchi sistemi.

Un modo consigliabile per iniziare la decrittazione si è quello di ricercare inizialmente le ripetizioni delle lettere o delle cifre nei crittogrammi derivati da una sostituzione, e le lettere a sequenze obbligate (come in italiano Q U) nei crittogrammi ricavati per trasposizione; oppure, dopo compiuto un attento esame del crittogramma, nel fare l'ipotesi dell'esistenza di una parola, di una frase o di una sequenza, presa tra quelle che con le maggiori probabilità vi sono comprese, e nel verificare poi l'esattezza dell'ipotesi fatta.

L'ipotesi naturalmente non è arbitraria ma è fondata sulla conoscenza della struttura dei vari sistemi di cifratura. Se l'ipotesi risulta esatta quasi certamente la decrittazione prosegue bene e riesce, perchè si è creata una falla nel crittogramma.

Le basi delle ipotesi vanno ricercate nelle frasi abituali, che in quasi tutte le corrispondenze si trovano al principio od alla fine, oppure nelle firme e negli indirizzi, tra i nomi di persone, di paesi, di cose, ecc., che l'argomento di cui tratta presumibilmente il crittogramma può far supporre; la verifica dell'ipotesi poi si può tentare operando sulle ripetizioni o sulle analogie che si riscontreranno nei crittogrammi disponibili, compilati con lo stesso sistema.

Il lavoro è certo arduo e pesante, ma non bisogna stancarsi dal ripetere ipotesi e verifiche.

Ogni sistema poi è caratterizzato da vari elementi particolari: relativi alla chiave, agli alfabeti usati, al raggruppamento per la trasmissione, ecc.; gioverà quindi ben stabilire quanti e quali sono gli elementi incogniti che occorre rintracciare per poter effettuare la decrittazione. Stabiliti questi elementi si passerà a definire entro quali limiti possono variare, in modo da restringere sempre più il campo delle ricerche.

Da quanto si è accennato appare dunque la capitale necessità pel decrittatore di studiare a fondo con quali caratteristiche particolari si presentino i crittogrammi ottenuti coi diversi sistemi, fino al punto di riconoscere senz'altro, esaminando semplicemente i crittogrammi, il sistema col quale sono stati cifrati; ma soprattutto lo studio deve condurre a conoscere le debolezze dei sistemi stessi per sapere da qual parte convenga iniziarne lo scardinamento.

Come si è accennato il lavoro di decrittazione molto si fonda sullo studio delle frequenze delle

singole lettere e sulle sequenze di più lettere nelle diverse lingue; vi sono quindi dei dati linguistici che occorre conoscere per bene compiere le operazioni crittografiche: tanto nel cifrare quanto nel decrittare. Daremo perciò un cenno di questi fondamenti linguistici della crittografia.

III. — *Dati sulle frequenze e sequenze letterali nelle varie lingue.*

I dati statistici relativi alle varie lingue che interessano la crittografia sono le frequenze e le sequenze, assolute e percentuali, nonchè le parole con significato concreto ed accessorio. Cerchiamo prima di chiarire cosa s'intenda con tali termini.

Il numero di volte che una lettera, o sillaba, o gruppo di lettere, o parola si trova nel brano che si esamina si dice *frequenza assoluta*, se questa si riferisce a 100 elementi si definisce *frequenza percentuale*.

La quantità dei casi in cui i predetti elementi si incontrano immediatamente a contatto di un altro elemento simile nel testo considerato si dice *sequenza assoluta*; anche di questa si ricava la *percentuale*. Le parti del discorso che significano una cosa, una qualità o una azione concreta, come sostantivi, aggettivi, verbi, si denominano in crittografia parole piene. Le parti del discorso che hanno invece nella lingua una funzione accessoria, come articoli, avverbi, congiunzioni, preposizioni, verbi ausiliari, ecc. si dicono parole vuote.

TABELLA

TABELLA delle frequenze delle lettere e dei

	1315 E	1160 I	1037 A	862 O	302 U	672 R	659 L	651 N	605 T	607 S
E	35	70	40	15	40	155	115	110	100	90
I	50	20	25	35	20	90	100	55	140	140
A	40	105	25	30	35	125	135	80	120	30
O	10	110	15	10	25	95	40	85	115	60
U	10	35	2	10	5	15	15	10	15	30
R	195	50	110	105	25	20	15	—	60	—
L	150	95	125	80	20	15	125	2	—	—
N	145	115	125	175	45	15	—	25	—	—
T	60	70	95	25	20	35	25	125	55	95
S	175	100	85	90	15	25	10	15	—	90
C	80	100	55	40	10	25	20	40	—	35
D	85	60	80	70	10	20	10	30	—	5
P	115	50	40	50	10	5	20	2	—	15
M	35	60	65	30	5	15	15	5	—	10
G	55	40	30	20	5	5	10	15	—	5
V	25	20	40	40	—	5	2	5	—	2
H	—	5	—	2	—	—	—	—	—	—
B	15	15	20	10	10	2	2	2	—	—
Z	5	5	30	—	—	5	—	40	—	—
F	10	25	15	15	2	—	—	5	—	—
Q	20	10	15	10	—	—	—	—	—	—

N. 1

bigrammi per la lingua Italiana, su 10.000 lettere.

437 C	377 D	315 P	257 M	210 G	152 V	107 H	95 B	94 Z	70 F	55 Q	
40	140	65	80	20	45	70	20	5	10	—	**E**
60	140	25	25	65	40	30	20	55	20	—	**I**
60	30	60	70	15	25	5	15	30	10	—	**A**
120	40	70	30	20	20	2	—	2	10	—	**O**
20	25	25	5	10	2	—	10	—	10	55	**U**
15	—	45	—	10	10	—	—	—	10	—	**R**
—	—	—	—	40	—	—	10	—	—	—	**L**
—	—	—	—	5	—	—	—	—	—	—	**N**
—	—	—	—	—	—	—	—	—	—	—	**T**
—	—	—	—	—	—	—	—	—	—	—	**S**
20	—	—	—	—	—	—	—	—	—	—	**C**
—	2	—	—	—	—	—	—	—	—	—	**D**
—	—	25	35	—	—	—	—	—	—	—	**P**
—	—	—	10	—	—	—	—	—	—	—	**M**
—	—	—	—	20	—	—	—	—	—	—	**G**
—	—	—	—	—	10	—	—	—	—	—	**V**
100	—	—	—	5	—	—	—	—	—	—	**H**
—	—	—	2	—	—	—	20	—	—	—	**B**
—	—	—	—	—	—	—	—	2	—	—	**Z**
—	—	—	—	—	—	—	—	—	—	—	**F**
2	—	—	—	—	—	—	—	—	—	—	**Q**

TABELLA delle frequenze delle lettere e dei

	1695 E	765 A	710 I	695 U	695 O	890 N	730 R	720 S	705 T	510 L	470 D	405 C	295 M
E	70	—	15	55	—	145	170	130	140	215	215	75	130
A	55	10	15	50	—	60	70	35	35	8[illegible]	80	55	20
I	10	70	—	55	70	20	75	80	115	35	55	10	55
U	90	55	—	—	180	20	20	55	30	30	55	40	10
O	—	—	70	—	—	70	80	40	35	30	15	95	40
N	260	120	70	90	190	80	—	10	30	15	—	—	—
R	130	130	50	100	75	10	20	10	80	—	30	15	—
S	280	20	55	60	50	110	20	40	30	—	—	—	—
T	115	70	120	55	10	170	50	55	20	—	—	15	—
L	110	60	50	15	10	10	55	40	35	70	—	—	—
D	140	10	30	10	10	55	30	90	90	—	10	10	—
C	80	30	10	40	20	70	30	55	—	—	—	30	—
M	135	30	20	30	40	—	20	15	10	—	10	10	10
P	80	55	—	40	10	—	30	20	15	—	—	—	30
V	40	50	15	35	10	15	30	10	—	—	—	—	—
F	35	10	10	20	—	15	10	10	—	—	—	—	—
B	—	20	—	10	10	10	—	—	—	—	—	—	—
G	20	15	30	—	—	—	10	—	—	—	—	30	—
Q	10	10	10	—	—	15	10	—	—	—	—	—	—
H	15	—	—	—	—	—	—	15	10	10	—	—	—
X	—	—	40	15	—	—	—	—	10	—	—	20	—
J	10	—	—	15	—	—	—	—	—	—	—	—	—
Y	—	—	—	—	10	15	—	10	—	10	—	—	—
Z	10	—	—	—	—	—	—	—	—	15	—	—	—
K	—	—	—	—	—	—	—	—	20	—	—	—	—
W	—	—	—	—	—	—	—	—	—	—	—	—	—

N. 2

bigrammi per la lingua Francese, su 10.000 lettere.

305 P	190 V	140 F	110 B	85 G	75 Q	60 H	65 X	15 J	50 Y	30 Z	K	W	
55	60	20	15	30	—	40	20	15	—	—	—	—	**E**
40	50	30	30	—	—	10	—	—	10	20	—	—	**A**
10	30	10	10	10	—	—	10	—	—	—	—	—	**I**
20	—	—	—	—	75	10	—	—	—	—	—	—	**U**
75	40	40	15	—	—	—	—	—	10	—	—	—	**O**
—	—	—	—	30	—	—	—	—	—	—	—	—	**N**
30	10	15	10	15	—	—	—	—	—	—	—	—	**R**
30	—	—	10	—	—	—	—	—	—	—	—	—	**S**
10	—	—	—	—	—	—	—	—	—	—	—	—	**T**
10	—	—	20	—	—	—	15	—	—	10	—	—	**L**
—	—	—	—	—	—	—	10	—	—	—	—	—	**D**
—	—	—	—	—	—	—	—	—	10	—	—	—	**C**
—	—	—	—	—	—	—	—	—	—	—	—	—	**M**
15	—	—	—	—	—	—	—	—	—	—	—	—	**P**
—	—	—	—	—	—	—	—	—	—	—	—	—	**V**
10	—	15	—	—	—	—	—	—	10	—	—	—	**F**
—	—	—	—	—	—	—	—	—	—	—	—	—	**B**
—	—	—	—	—	—	—	—	—	—	—	—	—	**G**
—	—	—	—	—	—	—	—	—	10	—	—	—	**Q**
—	—	10	—	—	—	—	10	—	—	—	—	—	**H**
—	—	—	—	—	—	—	—	—	—	—	—	—	**X**
—	—	—	—	—	—	—	—	—	—	—	—	—	**J**
—	—	—	—	—	—	—	—	—	—	—	—	—	**Y**
—	—	—	—	—	—	—	—	—	—	—	—	—	**Z**
—	—	—	—	—	—	—	—	—	—	—	—	—	**K**
—	—	—	—	—	—	—	—	—	—	—	—	—	**W**

TABELLA

TABELLA delle frequenze delle lettere e dei

	1265 **E**	825 **O**	790 **A**	675 **I**	300 **U**	150 **Y**	910 **T**	735 **N**	665 **R**	650 **S**	585 **H**	410 **D**	360 **L**
E	55	5	—	40	10	2	55	60	175	55	275	75	85
O	35	15	2	85	2	15	105	40	65	75	55	19	20
A	105	10	—	20	2	35	40	50	65	55	120	45	30
I	30	10	10	5	7	2	105	60	60	60	60	65	20
U	2	85	10	—	—	—	25	—	15	30	10	35	15
Y	20	—	15	—	—	—	35	10	15	5	5	7	35
T	65	40	135	95	15	20	55	115	75	100	15	65	10
N	115	190	200	150	50	—	2	10	20	15	2	2	—
R	190	125	80	30	50	5	40	5	10	10	10	10	7
S	120	35	80	85	50	15	30	60	40	60	—	10	10
H	20	7	5	—	—	7	350	10	10	50	—	15	5
D	145	5	35	10	5	10	5	145	20	5	2	2	20
L	30	30	70	30	25	—	15	15	15	10	5	5	40
C	70	15	35	55	5	2	5	50	10	20	—	5	—
F	40	130	15	10	7	5	5	15	2	15	2	10	10
M	60	50	35	15	—	7	7	5	20	5	7	15	2
P	40	15	11	2	20	5	5	10	5	40	—	7	7
W	40	20	2	—	—	10	15	10	—	10	5	10	7
G	15	10	10	10	2	5	—	55	15	5	2	5	—
B	10	10	25	5	15	2	7	7	2	15	—	5	5
V	25	15	15	25	25	2	—	2	10	—	—	—	—
K	10	—	2	—	7	—	—	—	10	2	2	2	—
X	20	2	—	7	2	—	—	—	—	—	—	—	—
J	—	—	2	—	—	—	—	—	—	—	—	—	—
Q	2	2	—	—	—	—	—	2	—	2	—	—	—
Z	—	—	.2	5	—	—	—	2	—	—	—	—	—

N. 3

bigrammi per la lingua Inglese, su 10.000 lettere.

295 C	280 F	265 M	215 P	150 W	135 G	120 B	100 V	40 K	35 X	15 J	10 Q	7 Z	
70	15	65	30	20	25	55	70	15	—	2	—	2	**E**
60	60	35	35	25	10	2	10	—	10	10	—	—	**O**
35	20	35	40	20	10	2	10	5	5	2	—	—	**A**
20	35	40	15	30	2	5	10	15	—	—	—	5	**I**
7	20	5	5	—	10	—	—	—	2	2	10	—	**U**
—	—	5	—	—	2	10	—	—	—	—	—	—	**Y**
15	40	5	10	7	7	2	—	—	7	—	—	—	**T**
—	2	10	—	7	10	—	—	5	—	—	—	—	**N**
10	25	10	40	—	25	2	—	—	—	—	—	—	**R**
2	10	5	10	2	10	5	—	2	—	—	—	—	**S**
55	5	—	5	30	15	—	—	—	—	—	—	—	**H**
—	5	—	—	5	—	—	—	—	—	—	—	—	**D**
10	10	—	15	—	2	35	—	—	—	—	—	—	**L**
5	10	—	—	2	—	—	—	—	—	—	—	—	**C**
—	15	5	—	—	10	—	—	—	—	—	—	—	**F**
—	10	20	—	—	—	—	—	—	—	—	—	—	**M**
—	2	20	10	—	2	—	—	—	10	—	—	—	**P**
—	—	2	2	5	2	—	—	—	—	—	—	—	**W**
—	—	—	—	—	—	—	—	—	—	—	—	—	**G**
—	2	5	—	—	—	—	—	—	—	—	—	—	**B**
—	—	—	—	—	—	—	2	—	—	—	—	—	**V**
2	—	—	—	—	—	—	—	—	2	—	—	—	**K**
—	—	—	—	—	—	—	—	—	—	—	—	—	**X**
—	—	2	—	—	—	2	—	—	—	—	—	—	**J**
—	—	—	—	—	—	—	—	—	—	—	—	—	**Q**
—	—	—	—	—	—	—	—	—	—	—	—	—	**Z**

TABELLA

TABELLA delle frequenze delle lettere e dei

	1405 E	1290 A	875 O	705 I	400 U	115 Y	755 S	700 R	635 N	555 L	470 D	435 T
E	45	60	60	80	170	30	120	160	45	75	215	80
A	40	40	30	75	25	25	95	160	55	210	70	120
O	10	10	—	105	10	10	40	80	105	60	80	75
I	—	20	5	—	5	—	65	70	75	30	65	80
U	20	30	—	5	—	—	30	10	20	5	10	10
Y	10	45	20	—	5	5	20	5	—	—	5	—
S	245	145	180	75	35	5	10	25	40	10	—	5
N	170	175	125	20	10	—	—	20	5	5	—	65
R	235	95	145	80	40	—	—	20	—	5	—	—
L	220	125	40	20	10	5	10	35	35	30	5	—
D	65	125	65	40	20	5	55	10	55	20	10	—
T	30	30	20	45	30	—	135	30	80	10	—	—
C	100	95	25	75	—	5	40	25	55	20	—	—
P	40	65	50	20	5	5	50	5	10	30	5	—
M	60	65	45	20	10	5	25	10	5	10	5	—
Q	10	45	10	5	5	5	25	20	10	10	—	—
B	10	45	25	5	10	5	5	—	5	—	—	—
G	30	20	5	10	5	—	5	5	10	20	—	—
H	20	20	10	—	—	—	10	—	5	—	—	—
F	10	10	5	10	5	5	10	—	5	—	—	—
V	10	10	10	5	—	—	5	10	5	5	—	—
Z	10	10	—	5	—	—	—	—	5	—	—	—
J	10	5	—	5	—	—	—	—	5	—	—	—
X	5	—	—	—	—	—	—	—	5	—	—	—

N. 4

bigrammi per la lingua Spagnola, su 10.000 lettere.

445 C	335 P	255 M	145 Q	105 B	100 G	95 H	65 F	65 V	35 Z	30 J	10 X	
50	75	40	—	20	10	20	10	25	—	5	—	**E**
60	60	65	—	20	30	45	10	10	25	10	—	**A**
115	65	45	—	5	20	20	5	20	—	5	—	**O**
110	25	60	—	35	5	10	25	10	—	5	—	**I**
35	30	—	145	5	30	—	5	—	—	5	—	**U**
—	—	—	—	—	—	—	—	—	—	—	—	**Y**
—	—	—	—	—	—	—	—	—	—	—	—	**S**
10	65	—	—	10	5	—	10	—	—	—	—	**N**
—	—	—	—	—	—	—	—	—	—	—	—	**R**
5	10	—	—	10	—	—	—	—	—	—	—	**L**
—	—	—	—	—	—	—	—	—	5	—	—	**D**
30	5	—	—	—	—	—	—	—	—	—	—	**T**
5	—	—	—	—	—	—	—	—	—	—	—	**C**
—	—	40	—	—	—	—	—	—	—	—	5	**P**
—	—	—	—	—	—	—	—	—	—	—	5	**M**
—	—	—	—	—	—	—	—	—	5	—	—	**Q**
—	—	5	—	—	—	—	—	—	—	—	—	**B**
—	—	—	—	—	—	—	—	—	—	—	—	**G**
25	—	—	—	—	—	—	—	—	—	—	—	**H**
—	—	—	—	—	—	—	—	—	—	—	—	**F**
—	—	—	—	—	—	—	—	—	—	—	—	**V**
—	—	—	—	—	—	—	—	—	—	—	—	**Z**
—	—	—	—	—	—	—	—	—	—	—	—	**J**
—	—	—	—	—	—	—	—	—	—	—	—	**X**

TABELLA

TABELLA delle frequenze delle lettere e dei

	1845 E	750 I	525 U	485 A	265 O	965 N	800 R	690 T	645 S	525 D	465 H
E	45	225	20	—	—	90	195	225	80	230	100
I	190	—	—	—	—	35	90	—	55	125	35
U	65	10	—	80	—	65	45	20	45	30	30
A	20	—	—	10	—	35	35	55	45	45	30
O	—	—	—	—	—	20	35	10	45	—	20
N	480	100	170	65	65	20	45	—	—	10	—
R	340	—	80	65	35	20	—	45	—	30	65
T	80	100	10	55	10	65	80	45	70	—	45
S	115	70	80	30	30	80	55	55	35	10	20
D	70	20	—	—	—	255	55	20	20	35	—
H	30	30	20	10	20	10	10	30	—	—	30
L	70	—	—	55	35	10	30	—	10	—	30
C	—	80	55	55	10	—	35	—	80	—	—
G	45	65	20	30	10	70	20	10	—	—	—
Z	30	—	—	—	—	20	—	90	80	—	—
M	55	30	30	20	10	—	30	—	10	—	10
B	65	10	10	10	—	35	—	20	10	—	10
W	35	—	—	—	10	35	10	10	10	—	20
F	30	10	30	—	20	10	—	—	10	—	10
K	20	—	—	—	—	30	—	—	10	—	10
V	20	—	—	—	10	20	—	55	—	—	—
P	20	—	—	—	—	20	20	—	10	10	—
J	20	—	—	—	—	20	10	—	20	—	—

N. 5

bigrammi per la lingua Tedesca, su 10.000 lettere.

340 L	310 C	305 G	245 Z	220 M	190 B	145 W	165 F	145 K	130 V	75 P	65 J	
55	—	160	80	20	100	30	35	55	55	—	45	**E**
45	—	—	30	20	20	35	—	—	30	10	—	**I**
35	—	10	20	—	10	30	20	10	—	—	10	**U**
70	—	20	10	30	20	30	20	—	—	—	10	**A**
10	—	10	—	30	—	20	10	10	35	10	—	**O**
—	—	—	—	—	—	—	—	—	—	—	—	**N**
—	—	20	—	—	30	—	20	20	—	35	—	**R**
—	—	—	65	10	—	—	10	—	—	—	—	**T**
20	—	—	20	—	—	—	—	10	10	—	—	**S**
20	—	—	—	30	—	—	—	—	—	—	—	**D**
—	265	10	—	—	—	—	10	—	—	—	—	**H**
45	—	35	10	—	10	—	—	20	—	10	—	**L**
—	—	—	—	—	—	—	—	—	—	—	—	**C**
20	—	10	—	—	—	—	10	10	—	—	—	**G**
—	—	10	—	—	—	—	—	—	—	—	—	**Z**
—	—	—	—	20	—	—	—	—	—	—	—	**M**
—	—	—	—	10	—	—	10	—	—	—	—	**B**
—	—	10	10	—	—	—	—	10	—	—	—	**W**
—	—	—	—	30	—	—	10	—	—	10	—	**F**
20	45	—	—	—	—	—	10	—	—	—	—	**K**
—	—	10	—	20	—	—	—	—	—	—	—	**V**
—	—	—	—	—	—	—	—	—	—	—	—	**P**
—	—	—	—	—	—	—	—	—	—	—	—	**J**

TABELLA delle frequenze delle lettere e dei bi-

	1209 **A**	992 **I**	986 **E**	781 **O**	397 **U**	645 **N**	634 **S**	544 **R**	452 **D**	403 **P**	373 **T**
A	6	30	5	—	6	220	78	110	142	61	75
I	36	15	25	15	15	115	55	65	20	—	90
E	4	15	—	—	—	85	70	144	30	45	40
O	53	25	63	15	5	90	15	90	32	110	50
U	9	10	20	—	5	40	65	40	35	15	10
N	125	115	125	46	35	15	36	5	55	5	—
S	95	210	95	60	60	10	5	10	20	19	5
R	80	45	50	56	15	5	20	—	80	110	50
D	90	25	135	130	25	5	—	—	5	—	—
P	104	15	55	50	19	—	45	10	5	5	24
T	55	20	85	30	30	10	130	5	—	5	—
J	41	82	20	105	20	30	—	—	—	—	5
V	116	15	30	65	16	5	31	—	11	5	15
M	35	154	45	50	15	—	—	—	12	—	4
K	83	43	75	45	10	—	55	5	—	15	5
Z	85	25	39	49	45	5	5	40	—	4	—
L	92	40	20	10	36	—	20	15	5	—	—
C	79	70	44	32	10	5	4	—	—	—	—
G	12	5	25	90	26	—	—	5	—	—	—
B	9	9	10	33	4	—	—	—	—	—	—
H	—	24	—	—	—	5	—	—	—	4	—
F	—	—	20	—	—	—	—	—	—	—	—

N. 6

grammi per la lingua Serbo-croata, su 10.000 lettere.

369 **J**	343 **V**	340 **M**	336 **K**	325 **Z**	314 **L**	220 **C**	182 **G**	80 **B**	45 **H**	20 **F**	
66	108	90	80	100	66	45	12	5	—	—	**A**
45	60	40	55	60	75	60	10	20	—	—	**I**
193	40	99	5	40	53	50	15	15	—	15	**E**
10	25	21	85	15	59	—	65	—	15	—	**O**
20	—	20	55	—	5	15	—	—	—	—	**U**
5	60	—	—	60	11	20	—	15	5	—	**N**
10	5	25	10	5	—	—	10	—	—	—	**S**
—	—	5	16	—	—	5	15	10	5	5	**R**
15	10	—	—	10	—	—	5	—	15	—	**D**
5	10	—	—	10	—	—	—	—	—	—	**P**
—	—	10	5	—	—	—	—	—	—	—	**T**
—	10	—	5	10	45	11	3	—	—	—	**J**
—	—	5	10	—	—	5	—	—	—	—	**V**
—	—	—	—	—	—	—	10	—	5	—	**M**
—	—	5	—	—	—	9	—	—	—	—	**K**
—	—	5	5	—	—	—	5	5	—	—	**Z**
—	10	5	5	10	—	—	27	10	—	—	**L**
—	—	—	—	—	—	—	—	—	—	—	**C**
—	5	6	—	5	—	—	5	—	—	—	**G**
—	—	4	—	—	—	—	—	—	—	—	**B**
—	—	—	—	—	—	—	—	—	—	—	**H**
—	—	—	—	—	—	—	—	—	—	—	**F**

Tabella delle frequenze e sequenze

lingue	lettera più frequente	Altre lettere più frequenti	Bigrammi più frequenti
Italiana	E (I-A-O)	L, N R, S, T	Er, Es, On, Re, De, Di, Ti, Si, El, En, La, Al, Nt, Ra, Co, Ta, To, Le, Li, An, In, Io, Ar, Or
Francese	E	N, A, R, S, I, T, U, O, L	Es, En, Le, De, On, Ou, Nt, Re, Ne, Se, El, Ai, Te, La, It, Er
Inglese	E (T)	O, A, I, N, R, S, H	Th, He, An, Er, On, Re, In, Ed, Nd, At, Of, Or, Ha, En, Nt, Ea, To, Ti
Spagnola	E	A, O, R, S, N, I, L, D	Es, En, El, De, La, Os, Ar, Ue, Ra, Re, Er, As, On, St, Ad, Ai, Or, Ta, Co, Se, Ac, Ec, Ci, Ia
Tedesca	E	N, R, I, T, S, A, U, D	En, Er, Ch, Nd, De, Te, Je, Ei, Un, Ge, Di, Es, In, He, Be, It
Serbo-croata.........	A	O, I, E, S, N, J, R, T	Je, St, Ni, Na, Os, An, Po, Pr, As, Av, Od, Ed, La, Aj, Ta, En, Ov, Ko, IJ, IS

più caratteristiche per ogni lingua

Trigrammi più frequenti	Sequenze obbligate	°/° della somma vocali	°/° somma consonanti più frequenti	Parole vuote più frequenti	Lettere rare
Che, Ere, Zio, Del, Que, Ari, Ato, Eco, Edi, Ide, Esi, Idi, Ero, Par, Nte, Sta, Men	Qu, Che, Chi, Ghe, Ghi	46	32	E, Che, A, Per, Di, In, Con, Ha, È, Ho	J, K, X, Y, W
Ent, Ede, Les, Que, Lle, Ait, Eme, Ion, Eur, Men, Nte, Est	Qu (Ux)	44	34	De, La, À, Et, Les, Le, Du, Que, Se, Par, Est	K, V
The, And, Tha, Hat, Edt, Ent, For, Ion, Nde, Tio, Has, Men, Sth	J e V con vocali	40	35	The, To, Of, A, In, And, Is, It, For, Has, On, Or, At	J, Q, Z
Que, Est, Ara, Ado, Del, Cio, Nte, Osa, Ede, Per, Ist, Nei, Res, Sde	Z, J, H, V con vocali; Qu	48	31	En, La, Que, De, Lo, Del, El, Los, Se, Y	K
Ein, Ich, Den, Der, Ten, Cht, Sch, Che, Die, Ung, Gen, Und, Nen, Des, Ben, Rch	Cu (Ch)	38	35	Die, Der, Und, Den, Zu, In, An, Ist, Dass, Es	Q, X, Y
Ste, Sta, Ijd, Jad, Smo, Str, Sve, Slo, Zna, Zno, Ako, Jak, Ski, Sko, Cki, Cko,	H preceduta da vocale o da J	42	30	Je, U, Na, A, I, O, Se, Su, Da, Ne, Is, Ce, Do, Ako	W, X, Y, Q

Prima di esporre i dati linguistici caratteristici di alcuni dei principali idiomi europei si può far osservare come tutti abbiano delle proprietà comuni, enunciabili come segue:

in brani di qualsiasi lingua, contenenti almeno 1000 lettere, possono ritenersi costanti:

la frequenza percentuale di ogni lettera;

le sequenze percentuali di ciascuna lettera con ciascuna delle rimanenti;

la frequenza percentuale di alcuni bigrammi e trigrammi, e quindi anche di alcuni dittonghi e trittonghi;

la frequenza percentuale della somma delle vocali;

la frequenza percentuale della somma delle consonanti più frequenti;

la frequenza percentuale delle parole vuote, e quella della loro somma (circa il 50%).

I dati sopra elencati si trovano comunemente raccolti e ordinati in tabelle od in grafici, e talvolta, come ad esempio fece il Gioppi nella precedente edizione di questo Manuale, si compilano elenchi delle principali parole della lingua, riunite secondo i gruppi, di 2, 3, 4 lettere più tipici e più frequenti nella lingua considerata.

Allo scopo di non dilungarci in una arida elencazione di dati numerici relativi a ciascuna lingua, diamo sintetizzati nelle tabelle annesse:

la frequenza delle lettere e dei bigrammi (tabelle 1 a 6;

le frequenze e le sequenze caratteristiche più importanti (tabella 7).

Consigliamo al lettore di fare un esame comparativo accurato delle tabelle, dal quale potrà trarre una somma di interessanti osservazioni.

Alcuni rilievi che non appaiono evidenti dalle tabelle li esporremo qui di seguito per ciascuna delle lingue considerate.

Lingua italiana. — Caratteristico è il raddoppiamento delle consonanti, quelle più frequentemente raddoppiate sono L, S, T, P, meno G e B.

Non si trovano quasi mai più di tre consonanti di seguito, se si incontra una simile sequenza di lettere, tra esse v'ha certamente una R, o una S, o una L.

Le sequenze delle altre vocali colla E sono meno frequenti delle sequenze della stessa lettera colle consonanti.

Lingua francese. — Non si trovano più di 5 consonanti senza vocali, nè più di 4 vocali di seguito.

Le lettere più frequenti che hanno maggiori sequenze con la E sono consonanti, raramente vocali.

La E si trova facilmente raddoppiata, le altre vocali di rado; le consonanti doppie più frequenti sono L, S, N.

Lingua inglese. — Le consonanti che presentano raddoppiamenti sono S, R, L; di rado le altre.

Lingua spagnola. — Le parole spagnole terminano in generale con una vocale oppure con S o con N.

Si incontrano raddoppiate soltanto L, R, C, e le vocali A, E.

Le sequenze più frequenti con la E sono date da consonanti.

Lingua tedesca. — In generale le parole terminano con una consonante. Sono rari i raddoppiamenti di vocale.

Le più frequenti sequenze con la E sono date da consonanti.

Lingua serbo-croata. — Si incontrano parecchie parole formate da 4 consonanti. Le parole straniere entrate nel linguaggio corrente vengono scritte come vengono lette nella lingua d'origine.

IV. — *Procedimenti particolari di decrittazione dei principali sistemi crittografici.*

Come si è detto non esistono regole generali e comuni per la decrittazione di tutti i sistemi, ma gli studi compiuti sulla particolare struttura di ciascuno di questi e la conoscenza delle particolarità delle varie lingue indicano le vie più redditizie da seguire per iniziare e condurre a buon termine questo lavoro. Vedremo perciò come si possa operare in particolare quando si voglia iniziare la decrittazione di un testo cifrato con un determinato sistema. Ricordiamo che in precedenza devono compiersi le ricerche relative alla lingua del crittogramma ed al sistema usato.

Decrittazione dei sistemi a trasposizione. — In questi sistemi le lettere che compongono il testo chiaro rimangono le stesse nel cifrato, quindi le varie frequenze percentuali restano identiche. La prima operazione da compiere quindi è il computo delle frequenze letterali, e delle conseguenti frequenze dei gruppi di lettere, della somma delle vocali e delle consonanti, ecc.

Questo lavoro preparatorio serve per lo sviluppo della operazione tipica per la decrittazione di questi sistemi, ossia per la ricerca delle lettere a sequenze obbligate, secondo le proprietà note di ciascuna lingua (vedi tabella 7). Questa ricerca riesce tanto meglio se si dispone di parecchi crittogrammi contenenti lo stesso numero di lettere, perchè siccome nei crittogrammi a trasposizione cifrati con la stessa chiave (egual numero di caselle) ed aventi la stessa lunghezza, ciascuna lettera del chiaro viene sempre ad occupare lo stesso posto nel testo cifrato, di conseguenza si potranno confrontare le sequenze delle lettere occupanti gli stessi posti nei vari crittogrammi ed averne norma nello scegliere l'ordine più probabile. Riusciti a trovare qualche sequenza possibile nella lingua chiara si tratterà di proseguire spostando con successivi tentativi le altre lettere per formare delle parole suggerite dalle sequenze trovate.

Nel caso si tratti di *trasposizione semplice* si cercherà di costruire il rettangolo per tentativi, dando vari valori al numero delle caselle orizzontali e verticali fin quando, giunti al rettangolo giusto si riuscirà a rintracciare il chiaro scritto in un ordine più o meno regolare, ma facilmente rilevabile. Sui crit-

togrammi a *trasposizione con chiave* a rettangolo completo si opera dapprima cercando di ricostruire il rettangolo, i cui lati potranno variare entro i limiti indicati da due numeri il cui prodotto sia eguale al numero delle lettere del crittogramma; ed ancora tali due numeri non potranno oscillare al di fuori di certe logiche possibilità di lunghezza di chiave. Fissati i rettangoli possibili, per trovare quello vero ci si basa sulla frequenza percentuale della somma delle vocali, che in ciascuna colonna ed in ciascuna linea non deve discostarsi troppo da quella caratteristica della lingua; i rettangoli con frequenze inammissibili sono senz'altro scartati.

In quelli che rimangono si prosegue basandosi sulle sequenze obbligate e sui poligrammi più frequenti, provando a cambiare l'ordine delle colonne fin quando si giunga a combinazioni soddisfacenti; trovata una disposizione di colonne che dia poligrammi possibili in tutte le linee la decrittazione si può dire ottenuta non presentando più alcuna difficoltà pel suo proseguimento.

Se la trasposizione con chiave è fatta a rettangolo incompleto la decrittazione presenta maggiori difficoltà poichè manca l'indicazione del prodotto dei due lati, e non tutte le colonne sono di eguale lunghezza. Un aiuto sensibile si ha in questo caso quando si conosca l'inizio o la fine del crittogramma, poichè si potrà quasi certamente stabilire la lunghezza e l'ordine della chiave.

Per la decrittazione dei crittogrammi *derivati da griglie quadrate* si procede fondandosi sul modo par-

ticolare, già visto, in cui sono costruite e sulle sequenze obbligate. Quando si tratti di griglie continue e si disponga di più crittogrammi di lunghezza presso a poco eguale si può operare nel modo indicato parlando in generale della decrittazione dei sistemi a trasposizione.

Quando si debbano decrittare testi cifrati con *doppia trasposizione* il lavoro si presenta con parecchie difficoltà; possiamo quindi considerarlo un metodo buono per la conservazione del segreto e lasciare allo studioso di escogitare quali possano essere le migliori vie da seguire pel raggiungimento dello scopo.

Decrittazione dei sistemi di sostituzione letterale. — Un sistema di sostituzione letterale si manifesta perchè le frequenze e le sequenze che vi si riscontrano sono differenti da quelle regolari del linguaggio comune. Però nei sistemi monoalfabetici i valori numerici delle frequenze e delle sequenze non cambiano, pur risultando attribuiti a lettere od a gruppi differenti da quelli del linguaggio chiaro, ciò naturalmente in dipendenza delle *sostituzioni letterali* effettuate; e perciò se dal computo delle frequenze letterali rilevate in un crittogramma si ricava un diagramma a valori decrescenti si ottiene un andamento simile a quello che si otterrebbe dal corrispondente testo chiaro. Questa osservazione viene utilmente sfruttata per il lavoro preparatorio della decrittazione.

Invece nei sistemi polialfabetici è tipica la uniformità delle frequenze e sono anche rare le ripeti-

zioni di sequenze molto lunghe; ciò è evidente quando si ricordi come si cifra con questi sistemi, nei quali la stessa lettera è ogni volta cifrata con un diverso alfabeto cifrante.

La decrittazione dei *sistemi monoalfabetici* si può ritenere sicura quando il crittogramma si componga di una quarantina di lettere. Il procedimento si fonda sullo studio delle frequenze e delle sequenze e sulla individuazione dei bigrammi e trigrammi più comuni nella lingua del testo originale. Si deve quindi fare il computo delle frequenze delle lettere del crittogramma e tradurlo in un diagramma in cui queste siano disposte in ordine decrescente (il diagramma si può costruire disponendo sull'asse orizzontale le lettere in ordine decrescente di frequenza e sull'asse verticale i valori delle frequenze rilevate). Questo diagramma si confronta con quello analogo della lingua normale, e dal confronto si possono dedurre quali lettere del crittogramma corrispondano alle più frequenti della lingua e quali alle meno frequenti.

Fatta questa prima separazione si procede alla ricerca delle vocali; è perciò necessario prepararsi un secondo diagramma delle sequenze delle varie lettere del crittogramma con la lettera più frequente dello stesso, anche questo diagramma si confronta con quello analogo della lingua chiara (che può essere ricavato dalle tabelle 1 a 6 che trovansi in principio di questo capitolo).

Le vocali così si possono individuare facilmente considerando i dittonghi più frequenti nella lin-

gua. Rintracciate le vocali si cercano i bigrammi ed i trigrammi più comuni, questi per tentativi e per induzione si completano con altre lettere fino a ricavarne delle intere parole e si giunge così con relativa facilità a ricostruire l'intero testo chiaro.

I crittologhi Kasiski, Kerckhoffs, Valerio e Bazeries hanno, in epoche diverse, studiato e proposto vari metodi di decrittazione dei *sistemi polialfabetici*, fondati sulle caratteristiche linguistiche e sulla struttura del sistema di cifratura.

In sintesi tali metodi derivano dai seguenti principî:

a) in qualsiasi testo cifrato poligrammi simili sono derivati da gruppi simili di lettere, cifrati con lo stesso alfabeto;

b) il numero delle lettere cifrate, contenuto nell'intervallo tra due poligrammi simili, è un multiplo del numero delle lettere della chiave; di conseguenza il divisore comune di tali multipli indica la lunghezza della chiave.

Ricavata così la lunghezza della chiave, ed insieme il numero degli alfabeti impiegati, resta da ricavare il loro ordine di successione.

Perciò disponendo di più crittogrammi cifrati colla stessa chiave, osservando che le lettere che occupano lo stesso posto nei vari testi cifrati sono derivate colla stessa chiave, se si scriveranno tutti i crittogrammi uno sopra l'altro con le lettere in colonna, avverrà che tutte le lettere della 1ª colonna saranno cifrate con la 1ª lettera della chiave, quella della 2ª colonna con quelle della 2ª lettera, ecc.

In altri termini tutte le lettere di una stessa colonna appartengono allo stesso alfabeto. Ed allora ogni alfabeto potrà essere decrittato, nel modo visto pei monoalfabetici, col computo ed il confronto delle frequenze e delle sequenze.

Se i vari alfabeti sono, per avventura, tutti derivati da quello regolare la decrittazione diviene molto facile, ed ancor più agevole se la chiave è corta ed è una parola usuale, anzichè essere dei tipi complessi da noi considerati.

Se invece gli alfabeti usati sono trasposti, e così pure le chiavi sono complicate con cura, la decrittazione si presenta più ardua ed occorre un forte numero di crittogrammi a disposizione per accingersi al lavoro con probabilità di successo.

Quando si sia proceduto molto innanzi nella decrittazione di uno di questi sistemi è possibile accingersi alla ricostruzione integrale della chiave e di tutti gli alfabeti; ma questa è un'operazione che rientra in quelle, cui accennavamo al principio del presente capitolo, che richiedono particolari abilità nel decrittare e pertanto non ci dilunghiamo in considerazioni ed in una esposizione, che pur potendo riuscire interessanti, escirebbero dai limiti e dai fini di questo manuale.

Decrittazione dei sistemi di sostituzione di gruppi di lettere. — Si è visto, trattando di questi sistemi di cifratura, che i bigrammi che si possono formare con le 26 lettere dell'alfabeto sono 676 ed i trigrammi sono 17.576; ma lo studio dei testi chiari

e delle frequenze dei poligrammi fa rilevare che in pratica non si impiegano nell'uso corrente più di 300 bigrammi e più di 1500 trigrammi; ed inoltre che le frequenze massime esistenti per tali poligrammi sono rispettivamente del 3% e dell'1%; inoltre evidentemente i testi cifrati derivati dai sistemi in discorso conterranno un numero di segni multiplo di 2 se cifrati con lettere, o di 3 se cifrati con numeri, se si usa la cifratura per bigrammi chiari; invece conterranno un numero di segni multiplo di 3 se cifrati con lettere o di 4 se cifrati con numeri nel caso si usi la cifratura per trigrammi chiari. Per chiarire questa osservazione si ricorda come, essendo appunto 676 i bigrammi e 17.576 i trigrammi possibili nella lingua chiara, quando si sostituiscano con gruppi cifranti costituiti con numeri (che sono soltanto 10) divenga necessario impiegare gruppi cifranti costituiti di 3 o di 4 cifre per poterne disporre nel numero sufficiente a dare i corrispondenti dei bigrammi o dei trigrammi letterali chiari. Questi rilievi servono a far riconoscere se un crittogramma è stato cifrato con uno dei sistemi di sostituzione di gruppi di lettere. Ed in particolare richiamiamo l'attenzione del lettore su questi esempi di analisi della struttura dei vari modi di ciframento perchè ben rimanga fissato nella sua mente come lo studio iniziale minuto dei vari metodi sia indispensabile a chi voglia coltivare la difficile arte della decrittazione.

La decrittazione di questi sistemi presenta una certa difficoltà e richiede un lavoro piuttosto lungo e paziente. Gli elementi principali per l'operazione

sono alcune osservazioni derivanti dal modo di formazione delle tabelle quadrate e dalla posizione reciproca delle lettere dei bigrammi cifranti in dette tabelle.

Infatti, specialmente quando per la formazione della tabella quadrata si usi una chiave, accadrà che si avranno nelle prime caselle lettere frequenti della lingua e nelle ultime si avranno lettere rare.

Notiamo poi che qualunque bigramma chiaro contenente una determinata lettera è cifrato con un altro bigramma nel quale non può essere compresa che una delle 8 lettere che si trovano sulla stessa linea o sulla stessa colonna della lettera chiara considerata; ogni lettera del cifrato non può quindi essere che una delle quattro lettere esistenti sulla stessa linea, oppure quella sottostante immediatamente alla lettera chiara cui corrisponde.

Ed ancora si verifica che invertendo qualunque bigramma chiaro si inverte il suo cifrato.

Il lettore potrà chiarirsi meglio questi rilievi riesaminando la tabella relativa al sistema detto *Playfhar cipher*, di cui al capitolo IV.

Tenendo quindi presenti queste osservazioni e quelle fatte circa i bigrammi più frequenti nella lingua, si potrà cominciare a cercare di ricostruire la tabella ed a determinare qualche bigramma chiaro, facendo l'ipotesi dell'esistenza di qualche parola che probabilmente esiste nel testo: questa ipotesi può essere stabilita avendo idea dell'argomento cui il crittogramma si riferisce e rintracciando qualche serie ripetuta di bigrammi identici, che può appunto far supporre la presenza di una parola frequente.

Anche nella decrittazione di questi sistemi conviene fare il computo delle frequenze dei bigrammi esistenti nel crittogramma, preparando una tabella quadrata avente il lato di 25 caselle; si scrivono quindi tanto sull'uno quanto sull'altro lato le lettere esistenti nel crittogramma disposte in ordine di frequenza decrescente, quindi nella casella all'incrocio di ciascuna verticale con ciascuna orizzontale si scriveranno i due numeri indicanti la frequenza con cui il bigramma, composto dalle due lettere considerate, si presenta nel crittogranma prendendo come 1ª lettera del bigramma una volta quella sulla verticale, ed una seconda volta quella sulla orizzontale, e come seconda l'altra lettera (rispettivamente sull'orizzontale e sulla verticale).

Si avranno così prontamente sott'occhio le frequenze con cui si presentano i vari bigrammi nel crittogramma e ne sarà facile il confronto con quelli chiari, onde derivarne il più probabile significato.

Decrittazione dei sistemi di sostituzione di lettere con frazionamento. — Questi sistemi, come il lettore ricorderà, hanno nella loro struttura caratteristiche differenti che riassumeremo quindi trattando partitamente di ciascuno.

Sistema Pollux. — I crittogrammi cifrati sostituendo i segni dell'alfabeto Morse si presentano sempre di una certa lunghezza ed i segni cifranti hanno una particolare distribuzione nel crittogramma di cui cercheremo di spiegare la ragione.

I segni Morse in un testo d'una certa lunghezza si presentano con la frequenza approssimativa del

50% per il punto, del 25% per la linea, del 25% per lo spazio, il punto e la linea si presentano frequentemente raggruppati a 2 a 2, a 3 a 3, a 4 a 4; mentre lo spazio si trova isolato, a meno che il cifratore non ne ponga alcuni di seguito per ingannare.

Quindi per decrittare si tratta di separare i segni cifranti che corrispondono al punto ed alla linea da quelli che corrispondono allo spazio; per ciò occorre preparare un computo delle frequenze e delle sequenze dei vari segni; stabilire quali sono quelli che rappresentano gli spazi (non aventi frequenze tra di loro); eliminarli dal crittogramma; tra i segni rimanenti (tenuti separati per gruppi come lo erano dai segni indicanti lo spazio) individuare quelli rappresentanti i punti, che saranno in un numero circa doppio di quelli corrispondenti alle linee; finalmente dare ai vari gruppi di segni (punti e linee) il loro significato letterale.

Questo lavoro di decrittazione non è molto difficile e può portare a risultati concreti.

Sistemi tipo Collon. — Si tratta di ricostruire i bigrammi cifranti e pertanto anzitutto bisogna ricercare il modo col quale è stata fatta la seriazione per la cifratura.

A questo si giunge per successivi tentativi, facendo ogni volta il computo delle frequenze per ognuno dei bigrammi risultanti. La serie giusta sarà quella nella quale il computo delle frequenze darà valori che più si avvicinano a quelli normali della lingua; poichè infatti, una volta ricostruiti i bigrammi, ci si trova di fronte a un sistema di sosti-

tuzione monoalfabetico, la cui decrittazione può essere tentata con probabilità di riuscita.

Sistemi tipo Delastelle. — La decrittazione di questi sistemi — bifido e trifido — è quanto mai laboriosa e talvolta anche impossibile, non riteniamo quindi nè utile nè necessario in questa sede esporre alcuni dei metodi impiegabili. Anche in questi casi il procedimento consiste nel tentare di scoprire il modo nel quale il testo chiaro è stato disposto in serie per la cifratura e poi passare alla ricostruzione della tabella cifrante. Come caratteristica di questi sistemi si può far rilevare che se due parole o gruppi di lettere abbastanza lunghi si ripetono nel testo chiaro a un intervallo che sia un multiplo esatto del numero di seriazione, daranno luogo a coppie (nel bifido) od a terne (nel trifido) di gruppi cifrati che si ripetono ad intervalli eguali rispettivamente alla metà od al terzo della lunghezza della serie.

Decrittazione dei sistemi a repertorio. — I crittogrammi cifrati con dizionari cifranti si possono riconoscere con una certa facilità, se non sono sopracifrati, pel fatto che se i dizionari stessi:

sono costituiti da gruppi aventi un numero variabile di lettere, i crittogrammi saranno trasmessi coi gruppi cifranti separati nella stessa forma nella quale si ricavano dal dizionario;

sono formati con gruppi cifranti di 5 lettere o numeri, i crittogrammi presentano delle ripetizioni di gruppi identici, corrispondenti alle parole o frasi più comuni della lingua;

sono formati con gruppi cifranti tutti eguali di 2 o di 3, o di 4 lettere ed i crittogrammi vengono trasmessi per gruppi dì 5 cifre (economia) si verificherà che il testo avrà un numero di segni multiplo di quello delle lettere contenute in ogni gruppo cifrante, si potrà quindi constatare anche qui la ripetizione di gruppi identici.

All'opposto i crittogrammi dedotti da un repertorio con sopracifratura presentano la caratteristica di non avere assolutamente alcuna ripetizione, se però si usa una sopracifratura di sostituzione dei tipi più semplici le ripetizioni si conservano ed è quindi facile dedurre, come nei casi precedenti, che si tratta di testi cifrati con dizionari.

Premettiamo subito che la decrittazione dei sistemi a repertorio non è un'impresa nè facile nè di sicura riuscita, a meno che si tratti di codici paginati, ed il lettore ne comprenderà la ragione ricordando come sono costruiti questi ultimi.

Per accingersi in generale ad operare su testi cifrati coi repertori è sempre necessario disporre di altri elementi che aiutino ad iniziare il lavoro di decrittazione, come potrebbero essere la conoscenza generica dell'argomento trattato o quella di una parte del testo chiaro, che può alle volte ricavarsi da brani di comunicazioni riprodotte sui giornali; un aiuto considerevole talvolta è dato dall'esistenza in uno stesso telegramma di tratti in chiaro e di tratti cifrati.

Poichè di codici paginati ne esistono diversi in commercio può essere interessante esaminare al-

cune maniere di tentare la decrittazione dei testi ricavati da quelli.

La decrittazione si basa su alcune osservazioni derivanti dalla struttura di tali cifrari.

In essi i gruppi cifranti sono costituiti di due parti: una variabile, cioè il numero della pagina, l'altra invariabile ossia il numero della riga corrispondente alla significazione chiara. Di più si verifica che le varie pagine contengono un numero assai diverso di gruppi frequenti nella lingua; in altri termini in ogni repertorio vi sono pagine che contengono molti gruppi frequenti, altre pochi, altre nessuno. Una terza osservazione si può fare circa la numerazione delle pagine che è progressiva, talvolta in ordine crescente, tal altra in ordine decrescente; il fatto che la numerazione non sia continua non porta incagli, poichè l'interessante è di rintracciare l'ordine delle pagine, la numerazione delle pagine si ricaverà esaminando quali numeri si incontrano nel crittogramma e quali invece non appaiono mai.

Avendo dunque ben presenti questi rilievi si comincerà ad analizzare attentamente il crittogramma e si vedrà che alcuni dei gruppi più frequenti hanno in comune una parte, che sarà quasi certamente il numero della pagina.

Scoperti parecchi di questi gruppi più frequenti contenuti nella stessa pagina, si potrà attribuire loro un significato probabile, dedotto da considerazioni fatte sulla materia trattata nel crittogramma o dalla loro posizione rispetto ad altri gruppi fre-

quenti. In questo studio aiuterà un esame fatto su un vocabolario o meglio ancora su di un dizionario cifrante, dal quale si potrà ricavare quali significati più verosimili possono attribuirsi a due parole comincianti con la stessa iniziale e poco distanti tra di loro nell'ordine alfabetico, poichè abbiamo detto che i tentativi successivi si fanno su serie di gruppi cifrati aventi in comune il numero della pagina.

Se poi il crittogramma è cifrato con uno dei codici che si trovano in commercio l'operazione è di molto facilitata perchè cercando tutte le parole che terminano con lo stesso numero, indicante la riga, non si potrà tardare a scoprire la pagina nella quale tali parole sono comprese; se si riesce a determinare la numerazione di una o due pagine del cifrario, il resto del lavoro diventa di una semplicità grandissima e la decrittazione può considerarsi in breve tempo compiuta.

Quando invece si debba tentare la decrittazione di corrispondenze cifrate con repertori intervertiti, dato la mancanza assoluta di qualsiasi relazione tra parole che si succedono alfabeticamente, si incontrano seri ostacoli per la riuscita.

Speranze di successo si hanno quando si possa lavorare su molti crittogrammi molto lunghi e per qualche fortuita circostanza si sia riusciti a venire in possesso di qualche pezzo di testo chiaro derivante da qualcuno di quei crittogrammi.

In questi casi si potranno fare dei confronti tra i vari testi cifrati per dedurne, con pazienti computi di frequenza sui gruppi ripetuti, quali possano es-

sere le principali parole vuote e quindi procedere per tentativi alla ricerca di parole che presumibilmente possono essere contenute nei crittogrammi, ispirandosi essenzialmente agli argomenti in essi trattati.

Ci troviamo qui di fronte a quei casi nei quali, come scrivevamo nella prima parte di questo capitolo, si rilevano le qualità particolari dei decrittatori, i quali, anzichè basarsi su regole di carattere generale, operano guidati dall'intuito, dalla pratica e giungono talvolta a risultati sorprendenti.

Quando infine si tratti di operare su crittogrammi derivati da repertori ai quali sia stata applicata la sopracifratura entriamo in un campo nel quale la semplice elencazione di tutti i vari casi e sottocasi che possono presentarsi in pratica porterebbe ad una trattazione talmente estesa e complessa che riuscirebbe di scarso interesse per la generalità dei lettori.

Basta quindi far rilevare come la decrittazione di testi cifrati con codici sopracifrati sia uno dei compiti più ardui e più brillanti ai quali possa accingersi un appassionato crittografo.

CAPITOLO VIII.

La scelta dei sistemi di cifratura. Avvertenze per il loro buon impiego

Nei capitoli precedenti si sono esaminati i principali sistemi crittografici nella loro intima struttura e successivamente si sono esposti dei concetti fondamentali circa la possibilità di decrittazione di tali sistemi.

Il lettore attento quindi, se avrà ampliato lo studio dei modi di cifrare con riflessioni, osservazioni e confronti, potrà a questo punto essersi formato delle idee sufficientemente esatte sulla bontà relativa dei vari sistemi esposti e sarà in grado, ove gli occorra, di decidere a quale di essi affidare il segreto della propria corrispondenza.

Riteniamo tuttavia opportuno raccogliere in questo capitolo, a guisa di conclusione, alcune norme che possano servire di útile indicazione nella scelta dei sistemi di cifratura da adottare a seconda del tipo di corrispondenza cui devono applicarsi e che servano di guida alle persone incaricate di ese-

guire le operazioni di cifratura, onde i testi cifrati presentino le maggiori possibilità di resistenza ai tentativi di decrittazione.

Tutti i sistemi crittografici potrebbero essere impiegati con affidamento di conservare il segreto, ma occorrerebbe che chi li applica fosse sempre abilissimo; ciò non avvenendo in pratica ne deriva che i sistemi consigliabili per l'impiego corrente si riducano a pochi.

Questa considerazione la possiamo in altri termini sintetizzare facendo ben rilevare come il cifrario più sicuro sia quello che è meglio adoperato, e qualunque cifrario sia debole quando sia male adoperato.

Per la scelta del sistema di cifratura da adottare il primo elemento da considerare è quello del tipo di corrispondenza al quale deve essere applicato.

Le corrispondenze cioè vanno considerate sotto i punti di vista della loro delicatezza, del tempo pel quale importa che rimangano assolutamente segrete e della loro lunghezza.

La delicatezza della corrispondenza evidentemente limita la scelta ai sistemi più resistenti, così pure la durata del periodo nel quale si vuole la garanzia che il segreto rimanga inviolato impone l'adozione di procedimenti crittografici capaci di resistere ai più ostinati e abili tentativi dei decrittatori.

La lunghezza dei testi da cifrare a sua volta influisce sulle decisioni in merito al tipo di cifratura,

poichè, come si è fatto ripetutamente notare, le ripetizioni di elementi cifrati, che possono essere ovviamente più abbondanti in testi lunghi, sono uno dei fattori più importanti per la buona riuscita dei tentativi di decrittazione.

Quindi potremmo, per rendere più comprensive le nostre conclusioni, classificare le corrispondenze che comunemente occorre di cifrare intorno ai tre tipi, da considerarsi come casi-limite:

corrispondenze di grandissima importanza di interesse generale, molto lunghe, e per le quali la garanzia del segreto deve mantenersi per tempo considerevole, magari fino a qualche anno;

corrispondenze importanti, che interessano soltanto determinati campi dell'attività sociale, di lunghezza normale, da conservarsi segrete per un tempo limitato, qualche settimana o qualche mese;

corrispondenze pur sempre importanti, ma molto brevi (tipo comuni telegrammi), che interessa rimangano segrete per qualche giorno al massimo.

Da tale classificazione potremo senz'altro dedurre che per le prime occorreranno i codici sopracifrati, per le seconde i codici intervertiti, con o senza sopracifratura, o qualcuno dei sistemi letterali più perfezionati, e per le ultime i codici intervertiti (per comodità) o qualcuno dei sistemi letterali, esclusi naturalmente i più ingenui.

Non abbiamo di proposito accennato ai codici paginati che si trovano in commercio, perchè non danno alcuna garanzia di sicurezza se attaccati da decrittattori anche mediocremente abili e perchè debbono piuttosto considerarsi come mezzi creati

allo scopo di realizzare una economia nella trasmissione dei telegrammi (in dipendenza della tassazione fatta dalle tariffe vigenti per i testi cifrati) o di mascherare semplicemente comunicazioni di limitatissimo interesse.

Ammessi tali criteri vediamo qualche maggior particolare circa la scelta definitiva dei sistemi.

I codici intervertiti, costruiti come si è detto trattando della loro struttura, debbono essere di lunghezza diversa a seconda del tipo di corrispondenza, che a sua volta dipende dal genere di attività che esplica l'organizzazione che deve adoperarli. I termini e le frasi di uso corrente variano in quantità appunto con tali attività. Certo che un codice molto voluminoso è più comodo da impiegare, ma se viene scoperto o trafugato richiede un grosso lavoro e una forte spesa per rinnovarlo.

I documenti per la sopracifratura, tabelle o procedimenti di trasposizione dei tipi esaminati, devono ad ogni modo essere cambiati di frequente perchè si abbia una vera garanzia di segreto.

Tra i sistemi letterali più resistenti si possono adottare i polialfabetici ad alfabeti trasposti molto irregolarmente, nei modi visti, oppure quelli a frazionamento di lettere. In tutti i casi quando si impieghino chiavi di cifratura è indispensabile che esse vengano scelte di una certa lunghezza, complicate e cambiate, mediante accordi tra i corrispondenti, molto spesso. Là dove l'importanza dell'organizzazione lo consenta è consigliabile l'uso di macchine per cifrare, affidandone la scelta a perso-

nale capace che le collaudi con esatto criterio crittografico.

Così pure la compilazione dei cifrari, e l'incarico di congegnare i sistemi letterali da usare, dovrebbero sempre essere affidati a persone che si siano dedicate allo studio della crittografia; il personale poi incaricato di eseguire materialmente le operazioni di cifratura deve essere convenientemente preparato e continuamente sorvegliato per evitare che commetta trascuratezze o si lasci trascinare coll'andar del tempo dalla forza dell'abitudine ad adoperare soltanto alcune voci dei codici, anzichè sfruttarne tutte le particolarità e tutte le possibilità.

Per adoperare bene qualunque sistema di cifratura è indispensabile anzitutto studiarlo con cura in tutti i suoi particolari di costruzione e se si tratta di un repertorio bisogna esaminarlo a fondo per rendersi esatto conto di tutte le combinazioni che consente di usare per cifrare, in modo da raggiungere il fine di cifrare parole o frasi chiare identiche sempre in modo differente, ciò per la ragione più volte detta che quanto più si eliminano le ripetizioni nei crittogrammi, tanto maggiore è la probabilità di difendersi dalle minacce della decrittazione.

Normalmente ogni cifrario, od ogni sistema letterale, comprende una prefazione nella quale sono date le norme pel suo uso, ma esistono anche delle regole che hanno valore generale per tutti i sistemi e che devono sempre essere tenute presenti da tutti

i cifratori. Ne indicheremo alcune aventi importanza capitale ai fini di non rendere vane le operazioni di cifratura. Per nessuna ragione si devono lasciare in un crittogramma tratti in chiaro e tratti cifrati. La spiegazione è ovvia quando si ricordi di quanta utilità sia per la decrittazione il conoscere l'argomento trattato nel crittogramma. Se poi si commettesse l'errore di lasciare in una stessa proposizione o periodo alcune parole in chiaro, il danno sarebbe ancora maggiore.

I testi chiari che devono poi essere cifrati devono essere compilati con particolari cure per ridurli alla minima indispensabile lunghezza, per eliminare tutte le ripetizioni di parole o di frasi, per introdurvi quante più abbreviazioni sia possibile, senza nuocere alla chiarezza del testo. Questi accorgimenti si giustificano rammentando come sia più facile rintracciare elementi per le decrittazione in testi lunghi, e pensando come le abbreviazioni si presentino nel testo cifrato con una fisionomia diversa da quella della corrispondente parola completa.

Nel cifrare si deve cercare di sfruttare tutti i modi che il sistema fornisce per tradurre in cifre le parole e le frasi; cioè usare bene gli omofoni e se anche il cifrario dà un solo gruppo come equivalente di un elemento chiaro non valersi sempre soltanto di quel gruppo, ma per esempio cifrarlo lettera per lettera, o sillaba per sillaba. Insomma sforzarsi di variare al massimo il ciframento nei limiti concessi dalla struttura del sistema.

Una avvertenza importante da aver presente è

quella di non usare nei crittogrammi sempre le stesse frasi, soprattutto quelle che di solito si impiegano al principio ed alla fine delle corrispondenze e quelle di uso comune; se per caso il cifratore ne trovasse nel chiaro dovrà adoperarsi per tradurle in cifre in modo che non siano riconoscibili.

Altra abitudine dannosa è quella di cifrare in principio o in fine del crittogramma le indicazioni relative alla organizzazione od alla persona mittente della corrispondenza. Queste sono indicazioni che si scoprono ben presto e che servono ai decrittatori per dedurne altri elementi. Se si è obbligati a mettere tali indicazioni dovranno i cifratori curare di mascherarle abilmente nei modi predetti.

Se il destinatario chiede spiegazioni su un crittogramma giunto incomprensibile, dovrà farlo con testo tutto cifrato e così pure le spiegazioni dovranno essere fornite completamente in cifra. È evidente infatti che se dati di questo genere cadessero in chiaro in possesso di chi ha l'interesse di insidiare il segreto, gli si fornirebbe un prezioso materiale di lavoro.

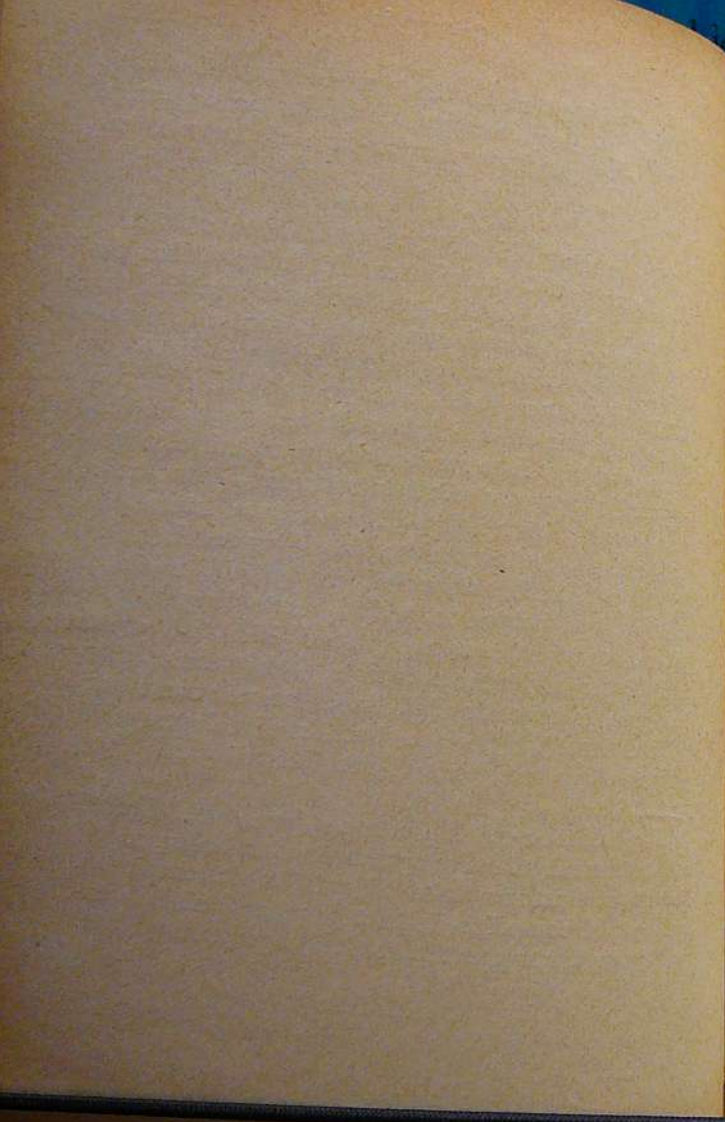
Particolare cura devono inoltre porre le organizzazioni che si valgono di corrispondenze in cifra ad evitare che siano eventualmente passate alla stampa, per comunicati, le traduzioni integrali chiare di testi cifrati; prima di far ciò si dovrà compilare un nuovo comunicato completamente diverso da quello ricavato dal testo cifrato.

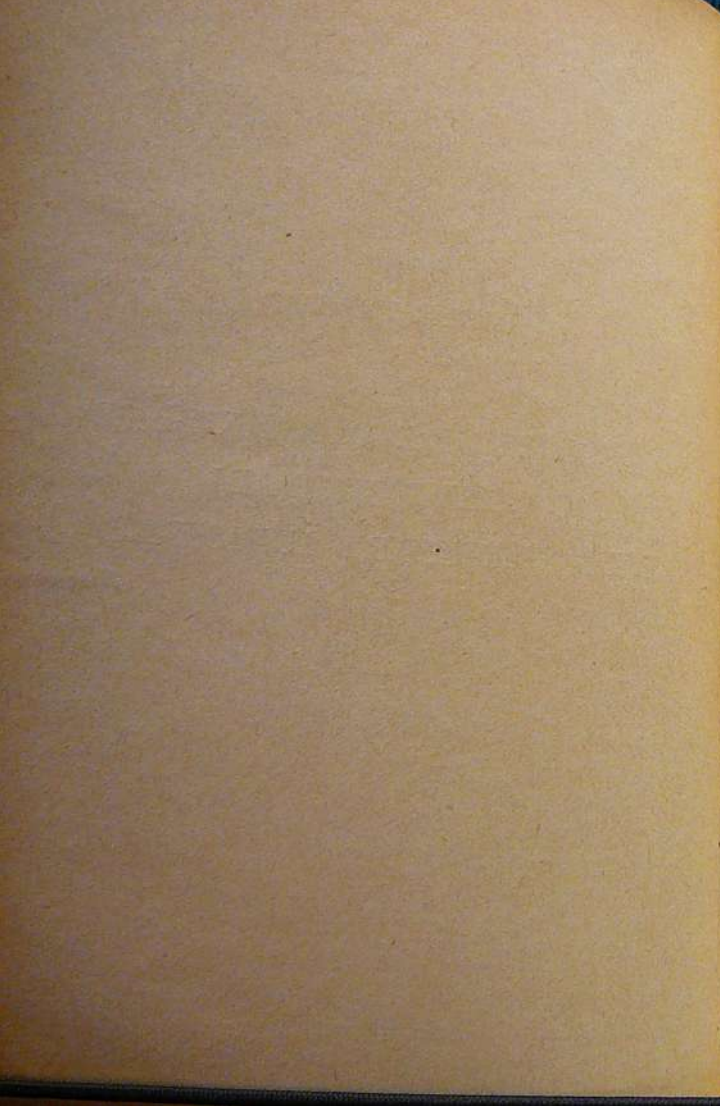
Da ultimo ricordiamo come non sia mai prudente comunicare ai vari corrispondenti i dati relativi ai

sistemi di cifratura da usare mediante testi cifrati, affidati al telegrafo con o senza filo, ma convenga invece farlo con lettere ordinarie e con tutte le garanzie.

Da quanto abbiamo esposto in questo capitolo riteniamo risulti sufficientemente chiarita l'importanza di servirsi delle operazioni crittografiche con costante serietà, se si vuole ottenerne risultati realmente efficaci. L'impiego della cifratura fatto con leggerezza è assai più dannoso che utile, perchè, nella presunzione di celare le nostre comunicazioni, può accadere che notizie delicatissime cadano invece in possesso degli interessati a conoscerle, precisamente per colpa della cifratura fatta male.

Quindi le organizzazioni che ricorrono alla crittografia per l'esplicazione delle loro attività è bene si valgano di personale tecnicamente preparato, e non di empirici, e soprattutto vigilino sulla onestà del lavoro di questo personale, sì che nessuna rilassatezza sia tollerata; delle indiscrezioni qui non parliamo perchè in tal caso si tratterebbe di veri reati, e non è questa la sede di considerare questa eventualità.

Da ultimo rammentiamo che per la compilazione e la tassazione dei telegrammi redatti in linguaggio segreto esistono delle disposizioni internazionali, che, per comodità del lettore, riproduciamo integralmente in appendice in fine del presente volume.

PARTE TERZA

LE SCRITTURE DISSIMULATE
O CONVENZIONALI
E LE SCRITTURE INVISIBILI

CAPITOLO IX.

Le scritture dissimulate o convenzionali

Secondo la classificazione delle scritture segrete che abbiamo stabilito al principio del presente manuale, un'altra delle maniere tipiche di occultare il contenuto delle corrispondenze è quella di impiegare un linguaggio che avendo tutti gli aspetti esteriori di quello chiaro, mascheri il suo reale significato.

Queste scritture possono presentarsi sotto la forma detta dissimulata o sotto quella detta convenzionale; le due forme di scrittura hanno struttura essenzialmente diversa.

Le *scritture dissimulate* consistono in procedimenti mediante i quali la comunicazione che si vuole dissimulare viene spezzettata e distribuita, inserita, frammezzo alle parole di una corrispondenza che presenta tutti i caratteri esterni di una comunicazione ordinaria qualsiasi. Lo spezzettamento e l'inserzione degli elementi della comunicazione segreta vengono eseguiti secondo accordi tra i corrispondenti, come vedremo in seguito.

Poichè evidentemente questa operazione richiede l'impiego di un testo piuttosto lungo per potervi inserire quello da dissimulare, ne deriva che il sistema si può sfruttare soltanto nelle corrispondenze epistolari, riuscendo difficile usare quelle telegrafiche in genere troppo brevi.

Le *scritture convenzionali*, pur avendo anche esse la proprietà di non distinguersi a prima vista da quelle ordinarie, sono compilate attribuendo alle parole che si trasmettono una significazione convenzionale, diversa da quella normale nel linguaggio chiaro, che viene stabilita tra i corrispondenti.

Le comunicazioni fatte con questo tipo di scrittura possono quindi essere di qualunque lunghezza; è ovvio come meglio si possano compilare se sono brevi, perchè presentano nel loro impiego il pericolo di destare sospetti sulla veridicità del loro contenuto; sono più frequentemente adoperate nelle comunicazioni telegrafiche.

Prima di trattare in particolare di questi sistemi facciamo rilevare come nella pratica non siano adoperati per le corrispondenze di carattere veramente delicato scambiate tra organizzazioni importanti, ma siano essenzialmente il mezzo di cui si valgono persone che devono occultare le proprie attività, talvolta anche poco oneste, oppure siano l'ingenuo sotterfugio per le corrispondenze di carattere sentimentale.

Sono in definitiva il linguaggio degli spioni, dei cospiratori e degli amanti.

In questo campo sono stati adoperati infiniti accorgimenti, qualche volta anche originali e geniali, ma noi ci limiteremo ad esporre soltanto qualche procedimento che presenta un certo interesse, specialmente quando si tratti di comunicazioni scambiate tra pochi corrispondenti.

Le scritture convenzionali. — Con queste scritture si può facilitare la trasmissione di notizie riguardanti fatti di un determinato ordine ben precisato, tra persone che non abbiano conoscenze dei metodi o che non possiedano codici di cifratura, o che non vogliano tenerne presso di sè. La limitazione degli argomenti che occorre trattare consente di concordare delle formule — tipo nelle quali ogni parola chiara, in quel determinato caso particolare, acquista un significato speciale.

In pratica si predispongono alcune frasi molto semplici relative alle notizie che si vogliono trasmettere e a ciascuna si fanno corrispondere altre frasi che sembrino comunicazioni riguardanti affari commerciali, notizie sportive, notizie famigliari, auguri, ecc. Queste ultime costituiscono il testo da trasmettere.

Così se i corrispondenti vogliono, a momento opportuno, inviare comunicazioni dei tipi qui di seguito indicati, potranno ad esempio usare formule del genere di quelle qui segnate:

1.º { Emissario giunto Bari con fondi.
Motore pronto garage completo.

2.º { Riunione lunedì casa Vallaro.
Provvedete bulloni, mm. . dodici

3.º { Scoperta spedizione distruggete opuscoli.
Augurando felicità gradite ossequii.

Come si vede questo sistema di corrispondere segretamente presenta scarso interesse dal punto di vista di un serio impiego della crittografia, ci sembra quindi sufficiente averne fatto cenno per una completa esposizione della materia.

Le scritture dissimulate. — Le maniere di dissimulare una comunicazione sono infinite, ma non ci occuperemo di quelle più ingenue e quindi di scarso valore pratico.

Un sistema, assai pericoloso se non ben applicato, è quello di segnare o scrivere in vario modo lettere o parole contenute in un testo a stampa (giornale o libro) od in una qualunque corrispondenza.

Da recenti studi pubblicati nel *Mercure de France* pare confermato che Lord Bacone abbia usato nelle sue opere un linguaggio dissimulato che si basava appunto sul diverso modo di stampare alcune lettere, le quali opportunamente combinate davano il testo segreto.

Poichè la questione è molto interessante ne daremo qualche particolare.

Il sistema di cifratura ideato da Bacone venne da lui stesso reso noto nell'opera in nove volumi « *De*

dignitate et augmentis scientiarum», pubblicata nel 1623.

Il sistema consta di due operazioni: la cifratura del testo chiaro da dissimulare; la dissimulazione del testo cifrato risultante in quello definitivo da pubblicare.

La prima cifratura del testo chiaro si eseguisce sostituendo ciascuna lettera con un gruppo cifrante di cinque lettere, secondo una tabella comprendente 24 disposizioni differenti ottenute con due lettere dell'alfabeto. Se le lettere impiegate sono la *a* e *b* si può avere ad esempio la seguente tabella:

A = a a a b a	N = a a b a a
B = a a a a b	O = b b a b b
C = a a a b b	P = a b b a a
D = a a b b b	Q = a b b b a
E = a b a b b	R = b b a b a
F = a b b a b	S = b a a a b
G = b b b b a	T = b a a b b
H = b b b a a	U, V = a a b a b
I, J = b b a a a	W = b a b b b
K = b a a a a	X = b a b b a
L = a b a b a	Y = a b a a b
M = b a b a b	Z = b a a b a

La seconda operazione, quella del dissimulare il testo derivato dalla prima cifratura, consiste nel sostituire le lettere dei gruppi cifranti con due alfabeti tipografici differenti, l'uno per le lettere che devono sostituire le *a*, l'altro per quelle che devono sostituire le *b*. I caratteri tipografici usati per le due lettere hanno differenze talmente lievi da non poter

essere rilevate da altre persone all'infuori di quelle a perfetta conoscenza del sistema.

Per chiarire il metodo poniamo di voler dissimulare la frase

tre son feriti

nel brano seguente:

«*L'atmosfera si presentava di una meravigliosa limpidezza, le montagne ancora illuminate....*»

La frase da dissimulare verrà nel testo da pubblicare stampata con caratteri tipografici corrispondenti alle lettere *a* e con caratteri tipografici corrispondenti alle *b*, nella maniera che qui sotto appare (per esigenze tipografiche però i caratteri corrispondenti alle *b* sono qui messi in *corsivo*).

t	r	e	s
b a a b b	b b a b a	a b a b b	b a a a b
*L*at*mo*	*sf*e*r*a	s*i*p*re*	*s*ent*a*
o	n	f	e
b b a b b	a a b a a	a b b a b	a b a b b
*va*d*iu*	na*m*er	a*vi*g*l*	i*o*s*al*
r	i	t	i
b b a b a	b b a a a	b a a b b	b b a a a
*im*p*i*d	*ez*zal	*e*mo*nt*	*ag*nea

Come appare evidente questo sistema richiede testi lunghissimi per dissimularne altri d'una certa lunghezza, ed infatti dai citati studi del Cartier, pubblicati nel *Mercure de France* negli anni 1921-22 apparirebbe come Bacone avesse impiegato questo

metodo per celare nelle sue opere particolari delicati e interessantissimi circa la storia d'Inghilterra, ai tempi della regina Elisabetta, e circa la personalità reale di Shakespeare.

Il metodo ideato da Bacone, modificato verso la fine dello stesso secolo XVII dal tedesco Federici, richiede inoltre pel suo impiego di potersi valere di mezzi tipografici, non è quindi alla portata di tutti.

Altri metodi invece possono essere adoperati colla scrittura ordinaria, derivandoli da quelli a frazionamento di lettere visti nel capitolo IV; per dissimulare cioè una corrispondenza si può prima cifrarla con uno di questi metodi e poi dissimulare il testo cifrato così ricavato in una lunga missiva dall'aspetto comune, nella quale si conviene, per esempio, che il numero delle consonanti, o delle vocali, contenute in ciascuna delle parole che compongono la missiva indichi un segno cifrante.

Ossia si cifra il testo da dissimulare prima, per esempio, colla tabella numerica del sistema Delastelle trifido o col Pollux (coi segni Morse) e poi si prepara una corrispondenza nella quale le successive parole contengono tante vocali (o consonanti) quante sono indicate dai numeri costituenti i vari gruppi cifranti. Il lettore potrà colle cognizioni ormai acquistate provare ad applicare questo sistema e si accorgerà che per dissimulare una frase occorrono tante parole quanto è il numero delle lettere della frase moltiplicato per tre.

Sistema di semplice uso, ma alquanto lungo e

noioso perchè si devono trovare parole del testo-base che contengano il numero di lettere necessario a rappresentare esattamente i segni cifranti. Il lavoro tuttavia non è difficile se si scrive prima senza alcuna preoccupazione il testo-base (quello cioè da trasmettere definitivamente) e poi lo si corregge, cambiandone alcune parole, a seconda delle necessità di rappresentazione dei segni della prima cifratura.

Il lavoro si può variare valendosi di un altro metodo che consiste nell'attribuire, per esempio, il valore 1 alle parole del testo-base che contengano un numero dispari di vocali (o di consonanti) ed il valore 2 alla parole che ne contengono un numero pari; poi nel preparare una tabella di equivalenza nella quale alle 16 combinazioni dei numeri 1 e 2 presi quattro a quattro corrispondano 16 lettere qualunque dell'alfabeto;

B	C	D	F	G	H	L	M	N	P	Q	R	S	T	V	Z
1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2
1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
1	1	2	2	1	1	2	2	1	1	2	2	1	1	2	2
1	2	1	2	1	2	1	2	1	2	1	2	1	2	1	2

Colle 16 lettere poi combinate due a due si ottengono 256 bigrammi, a ciascuno dei quali si fa corrispondere una parola o frase, costituendo così un piccolo codice cifrante.

Quando si voglia dissimulare una corrispondenza la si prepara valendosi delle parole o frasi contenute nel codice, la si traduce quindi nei bi-

grammi corrispondenti e questi, lettera per lettera, si dissimulano in una corrispondenza ordinaria nella quale il numero pari o dispari delle vocali (o consonanti) di ciascuna parola indicherà successivamente i numeri costituenti i gruppi cifranti, derivati dalla prima tabella numerica, equivalenti a ciascuna lettera dei bigrammi contenuti nel codice. A maggior chiarimento vediamo una applicazione pratica.

Sia quella sopraindicata la tabella numerica da usare e sia da dissimulare la frase « *Allontanatevi subito* ».

Nel codice preparato d'accordo tra i corrispondenti alla parola «allontanatevi» corrisponde il bigramma D R; alla parola «subito» corrisponde il bigramma T F, cioè la frase da dissimulare subirà le seguenti trasformazioni:

1.ª =	Allontanatevi		subito
2.ª =	D R	=	T F
3.ª =	1121 = 2122		1122 = 2212

quest'ultimo è il crittogramma da dissimulare in parole nelle quali il numero di vocali dispari indica l'1 e quello pari il 2; quindi potremo avere una corrispondenza definitiva da spedire così compilata:

Io so quanto tu devi soffrire dato questo lungo
1 1 2 1 2 1 2 2 2
periodo di dolorosa ansia che turba tanto...
2 1 2 1 1 2 2

Come ognun vede, in questo campo delle scritture dissimulate l'astuzia e l'intelligenza umana

possono ampiamente sbizzarrirsi in mille maniere, lasciamo quindi l'argomento che non ha interesse preminente nell'ambito delle attività nelle quali le scritture sono applicate per alti fini, ai quali meglio si addicono i sistemi crittografici a fondamento scientifico, quali quelli esaminati nel capitolo IV.

CAPITOLO X.

Le scritture invisibili

Fra le scritture segrete occupano un posto non trascurabile quelle invisibili, ossia quelle ottenute con gli inchiostri così detti simpatici, che hanno la proprietà di non divenire visibili se non sottoposti ad una particolare reazione fisica o chimica: riscaldamento, immersione, ecc.

Non indicheremo qui gli innumerevoli prodotti semplici o composti che possono servire come inchiostri simpatici, e le relative reazioni per rivelarli, poichè esistono molte pubblicazioni che si occupano della materia, come il *Ricettario domestico* del Ghersi e *Reattivi e reazioni* del Tognoli nei Manuali Hoepli, l'opera *Les Chiffres secrets dévoiles* del Bazeries, edita nel 1901 dalla casa Fasquelle a Parigi, ed altre ancora.

Esporremo invece dei concetti generali su tali scritture e sui mezzi di ottenerle, di guisa che il lettore nell'eventuale scelta di questi sappia procedere con criteri razionali.

Le scritture eseguite con inchiostri invisibili hanno lo scopo di nascondere ad occhi indiscreti il contenuto della corrispondenza ed hanno indubbiamente il vantaggio, se impiegate con conoscenze estese delle loro possibilità, rispetto alle altre scritture segrete di non destare sospetti per la loro apparenza come le scritture cifrate o per la ambiguità del testo che le dissimula se trattasi di scritture convenzionali o dissimulate.

Le scritture invisibili possono vergarsi sulla carta, sulla tela, sul legno, ecc., scegliendo un adatto inchiostro simpatico.

Gli inchiostri simpatici sono generalmente composti da un inchiostro propriamente detto, e da un reagente o rivelatore che serve a rendere visibile la scrittura e che può essere un prodotto chimico o un agente fisico, come la luce ed il calore.

L'inchiostro può essere una sostanza semplice od anche la mescolanza di più sostanze, per praticità d'impiego deve però formare un composto unico: il rilevatore invece può essere un composto da usarsi con una unica operazione, oppure essere costituito da diversi prodotti da usarsi successivamente

Le caratteristiche principali di un buon inchiostro simpatico sono la perfetta invisibilità dello scritto che ne risulta, prima ch'esso sia sottoposto all'azione del rivelatore, e la proprietà di non corrodere la carta, od altra sostanza, sulla quale viene eseguito lo scritto.

L'inchiostro poi evidentemente non deve potersi rivelare con grande facilità, il sugo di limone, il sale ammoniaco, l'acido solforico sono ad esempio mezzi

di scarso valore, perchè colla semplice azione del calore si rendono evidenti.

Quindi nello scegliere un inchiostro simpatico occorrerà limitarsi a prodotti che richiedano un rivelatore di difficile applicazione e possibilmente che sia lo specifico di tale prodotto.

Una differenza sostanziale tra l'inchiostro ed il rivelatore si è che mentre il primo deve poter essere usato con molta semplicità di mezzi, il secondo deve richiedere operazioni anche di una certa complicazione, perchè di solito chi scrive la comunicazione da occultare non ha tutte le comodità per operare, come invece le ha chi deve eseguire le operazioni per rivelare lo scritto.

Il rivelatore è bene anche che lasci traccia del suo impiego, per esempio alterazione del colore della carta, di modo che, se la corrispondenza segreta è stata manomessa, ne rimarrà il segno evidente.

Per la buona applicazione di una scrittura invisibile ha altresì grande importanza la scelta della carta da usare. Il miglior modo di effettuare tale scelta è quello di fare delle prove coll'inchiostro che si è deciso di adoperare su varie qualità di carta. — La carta, colla scrittura invisibile vergata, verrà poi sottoposta anche all'azione del rivelatore; attenzione particolare bisogna prestare al modo col quale la carta si presenta dopo essere stata bagnata, poichè quasi con tutti i rivelatori essa deve essere almeno inumidita e per usare molti inchiostri la carta deve essere preventivamente bagnata.

Da queste varie prove si ricaveranno sicure in-

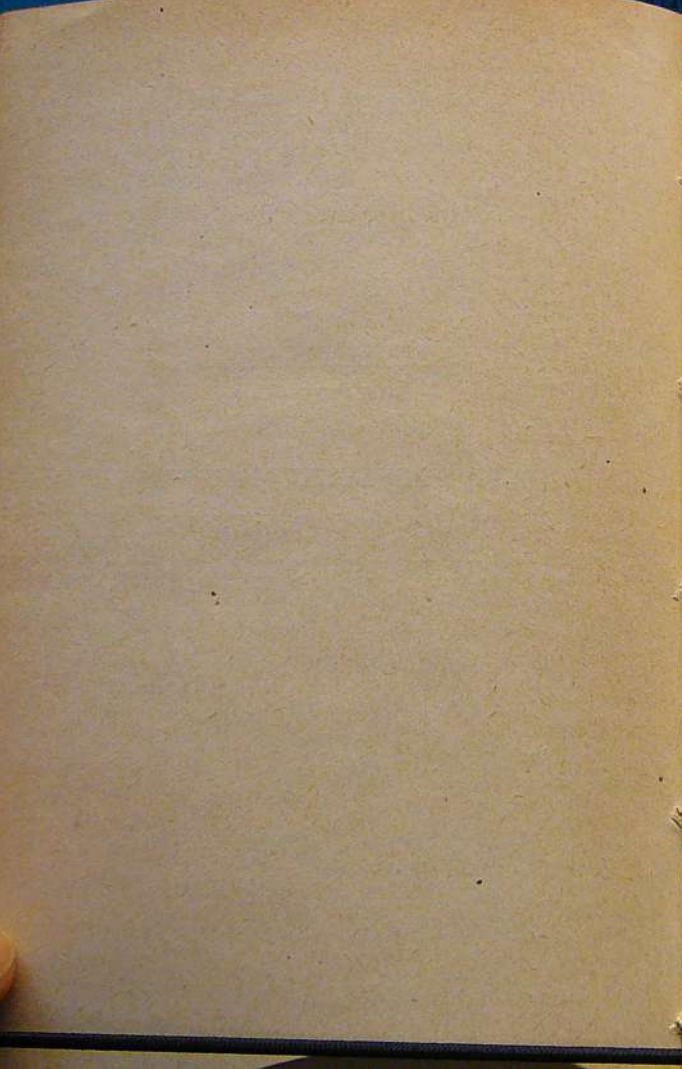
dicazioni sulle qualità da prescegliere, che facilmente si trovano in commercio.

I pennini che si usano normalmente per scrivere però alterano la superficie della carta, è perciò necessario scegliere anche questi con qualche cura. — Meglio di tutto servono steccoli di legno, ma anche i pennini d'acciaio possono essere usati, devono però avere molta elasticità, le punte arrotondate e rovesciate all'insù. L'elasticità si può migliorare arroventando le punte; i pennini devono essere impiegati sempre nuovi ogni volta che si scrive. Prima di accingersi a scrivere è bene bagnare abbondantemente la carta con acqua per toglierne la patina lucida che di solito esiste e perchè l'inchiostro simpatico aderisca meglio, quasi più per assorbimento che per pressione; nell'eseguire questa operazione bisogna cercare di ottenere la massima uniformità e non lasciare depositare l'acqua in alcun punto.

Per eseguire la scrittura, dopo aver effettuata la bagnatura della carta, si deve prima scrivere coll'inchiostro simpatico nel senso della altezza del foglio, lasciando un conveniente margine e scrivendo da una parte sola del foglio, bisogna cercare di tenere la mano molto leggera ed usare molta attenzione al fine di dare grossezza uniforme ai caratteri.

Poi si scrive la comunicazione coll'inchiostro ordinario nel senso della larghezza del foglio, senza alcuna particolare preoccupazione, anzi badando a che la missiva abbia l'aspetto il più normale possibile.

APPENDICE

DISPOSIZIONI INTERNAZIONALI RELATIVE AI TELEGRAMMI REDATTI IN LINGUAGGIO SEGRETO

Le varie conferenze telegrafiche internazionali, riunite allo scopo di elaborare le convenzioni universali destinate a garantire la sicurezza e la rapidità delle trasmissioni dei telegrammi in tutti i Paesi, hanno fissato, tra le altre, norme relative alla compilazione ed alla tassazione dei telegrammi compilati in linguaggio segreto.

La prima di tali conferenze fu riunita a Parigi nel marzo 1865, portò alla firma della Convenzione telegrafica internazionale del maggio 1865, stipulata fra venti Stati, venne in varie riprese modificata e completata in seguito alle conferenze tenute a Vienna nel 1868, a Roma nel 1872, a Pietroburgo nel 1875, a Londra nel 1879, a Berlino nel 1885, a Parigi nel 1890, a Budapest nel 1896, a Londra nel 1903, a Roma nel 1906, a Lisbona nel 1908, a Londra nel 1912, a Madrid nel 1920 ed a Parigi nel 1925.

La conoscenza delle norme relative ai telegrammi compilati in linguaggio segreto è indispensabile al duplice scopo della scelta dei segni pel ciframento e di quella del linguaggio da impiegare.

Riproduciamo perciò qui di seguito, tradotte in italiano, le principali norme circa tale materia, esse sono tratte dalla pubblicazione ufficiale del Ministero delle Comunicazioni. — Direzione generale delle poste e dei telegrafi. — Serv. Telegrafi, Div. I, che porta per titolo: « Convenzione telegrafica internazionale di Pietroburgo, approvata con R. D. n. 3163 del 1° giugno 1876 e Regolamento telegrafico internazionale (Revisione di Parigi) approvato con R. D. n. 1507 del 13 agosto 1926 » Roma, Provveditorato Generale dello Stato — Libreria, 1927.

CAPITOLO IV.

Art. 7.

1. — Il testo dei telegrammi può essere redatto in linguaggio chiaro o in linguaggio segreto, quest'ultimo si distingue in linguaggio convenzionale e in linguaggio cifrato. Ciascuno di questi linguaggi può essere impiegato solo o unitamente cogli altri in uno stesso telegramma.

2. — Tutte le Amministrazioni accettano, in tutte le loro relazioni, i telegrammi in linguaggio chiaro. Esse possono non ammettere nè alla partenza, nè all'arrivo i telegrammi privati redatti totalmente o parzialmente in linguaggio segreto, ma esse devono lasciare circolare questi telegrammi in transito, salvo i casi di sospensione definiti all'art. 8 della Convenzione.

Art. 8.

2. — Si intendono per telegrammi in linguaggio chiaro, quelli il cui testo è interamente redatto in linguaggio chiaro. Tuttavia l'esistenza di indirizzi convenzionali, di marchi di commercio, di corsi di borsa, di lettere rappresentanti i segnali del Codice internazionale, di segnali impiegati nei telegrammi marittimi, di espressioni abbreviate d'uso corrente nella corrispondenza ordinaria o commerciale, come *fob*, *cif*, *caf*, *svp* o qualsiasi altra analoga il cui apprezzamento spetta al Paese che spedisce il telegramma, di una parola di controllo situata all'inizio del testo nei telegrammi di banca o analoghi, non muta il carattere d'un telegramma in linguaggio chiaro.

Art. 9.

Linguaggio convenzionale

1. — Il linguaggio convenzionale è quello che si compone di parole che non formano frasi comprensibili in una o più tra le lingue autorizzate per la corrispondenza telegrafica in linguaggio chiaro.

2.— Le parole reali o artificiali devono essere formate da sillabe che possano pronunciarsi secondo l'uso corrente di una delle lingue tedesca, inglese, spagnuola, francese, olandese, italiana, portoghese o latina. Le parole artificiali non devono contenere le lettere accentate *ă*, *á*, *à*, *é*, *ñ*, *ö* *ü*.

3. — Le parole del linguaggio convenzionale non possono avere una lunghezza superiore a dieci

caratteri secondo l'alfabeto Morse; le combinazioni *ae, aa, ao, oe, ue*, sono contate ciascuna per due lettere. La combinazione *ch* è ugualmente contata per due lettere nelle parole artificiali.

5. — Le combinazioni che non soddisfano alle condizioni dei due paragrafi precedenti sono considerate come appartenenti al linguaggio in lettere avente significato segreto e sono tassate in conseguenza. Tuttavia quelle formate mediante la riunione di due o più parole del linguaggio chiaro contraria all'uso della lingua non saranno ammesse.

Art. 10.

Linguaggio cifrato

1. — Il linguaggio cifrato è quello che è formato:

1.° sia da cifre arabiche, da gruppi o da serie di cifre arabiche aventi un significato segreto; sia da lettere (escluse le lettere accentate *ă, á, à, é ñ, ö, ü*), da gruppi o da serie di lettere aventi un significato segreto;

2.° da parole, nomi, espressioni o riunioni di lettere non rispondenti alle condizioni del linguaggio chiaro (art. 8) o del linguaggio convenzionale (articolo 9).

2. — La mescolanza in uno stesso gruppo di cifre e di lettere aventi un significato segreto non è ammessa.

3. — Non sono considerati aventi un significato segreto i gruppi indicati all'art. 8, n. 2.

CAPITOLO VII.

Computo delle parole

Art. 2.

4. — Nel linguaggio convenzionale la massima lunghezza di una parola è fissata a dieci caratteri computati secondo le prescrizioni dell'art. 9, n. 3.

Le parole in linguaggio chiaro inserite nel testo di un telegramma misto, cioè composto di parole in linguaggio chiaro e di parole in linguaggio convenzionale, sono contate per una parola fino alla concorrenza di dieci caratteri, l'eccedenza è contata per una parola per serie indivisibili di dieci caratteri.

Se un telegramma misto comprende, inoltre, un testo in linguaggio cifrato, i passaggi in linguaggio cifrato sono contati conformemente alle prescrizioni del seguente n. 7.

Se un telegramma misto non comprende che passaggi in linguaggio chiaro e passaggi in linguaggio cifrato, i passaggi in linguaggio chiaro sono contati secondo le prescrizioni del n. 3 di questo articolo, e quelli in linguaggio cifrato secondo le prescrizioni del seguente n. 7.

7. — I gruppi di cifre o di lettere, i marchi di commercio composti di cifre e di lettere sono contati come altrettante parole per quante volte contengono cinque cifre o lettere, più una parola per l'eccedenza. Ciascuna delle combinazioni *ae*, *aa*, *ao* *ue*, *ch*, è contata per due lettere.

Sono contate come una cifra o una lettera nel gruppo dove essi figurano· i punti, le virgole, i due punti, le lineette, e le sbarre di frazione. — Lo stesso avviene per le lettere o le cifre aggiunte a un numero di abitazione in un indirizzo, anche se si tratti di un indirizzo che figura nel testo o nella firma di un telegramma.

8. — Le riunioni o alterazioni di parole contrarie all'uso della lingua non sono ammesse; lo stesso dicasi quando le riunioni o alterazioni sono dissimulate per mezzo dell'inversione dell'ordine delle lettere o delle sillabe.